UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------x

UNITED STATES OF AMERICA,

v. 23 Cr. 430 (KPF)

ROMAN STORM,

Defendant. Argument

----------x

New York, N.Y.
July 12, 2024
10:00 a.m.

Before:

HON. KATHERINE POLK FAILLA,

District Judge

APPEARANCES

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
BY: NATHAN M. REHN
BEN ARAD
BENJAMIN A. GIANFORTI
Assistant United States Attorneys

KEVIN G. MOSLEY
Special Assistant United States Attorney

WAYMAKER LLP
Attorneys for Defendant
BY: BRIAN E. KLEIN
KERI CURTIS AXEL
KEVIN M. CASEY

HECKER FINK LLP
Attorneys for Defendant
BY: DAVID E. PATTON

(In open court; case called)

THE DEPUTY CLERK: Please state your name for the record, beginning with the government.

MR. REHN: Good morning, your Honor. AUSA Thane Rehn, appearing for the United States. I am joined at counsel's table by AUSAs Benjamin Gianforti and Ben Arad, and Special AUSA Kevin Mosley.

THE COURT: Good morning to each of you and thank you very much.

Mr. Rehn, is it you to whom I should be directing my questions this morning or someone else?

MR. REHN: Primarily, your Honor. I will be handling the motions to dismiss and any scheduling issues. Mr. Gianforti will be addressing any questions you may have about the motion to suppress. And Mr. Arad will be addressing any questions you may have about the motion to compel.

THE COURT: Thank you.

My friends at the back. Thank you very much.

Mr. Storm, good morning to you, sir.

THE DEFENDANT: Good morning, your Honor.

THE COURT: If you could let me know if there is a division of labor with respect to oral argument today.

MR. KLEIN: There is, your Honor. Brian Klein appearing for Mr. Storm, who is here. With me is Keri Axel and Kevin Casey. And David Patton just joined; he filed a notice

of appearance yesterday.

THE COURT: Mr. Patton, welcome. Long time no see.

MR. KLEIN: We are dividing it up in a slightly different way than they are.

I am going to argue the motion to compel, the 1960 portion of the motion to dismiss, and discuss all of the scheduling and other matters. Ms. Axel is going to discuss the motion to suppress, the money laundering and IEEPA counts. And just to be full employment on this side, Mr. Casey, if you have any questions about due process or First Amendment on the motion to dismiss.

THE COURT: Okay. Thank you.

For those of you who have not had an oral argument before me, I will give you the advice I give to everyone. Please listen carefully to my questions. Don't read too much into them. They are not designed to signify anything other than my interest in exploring these issues. It is often the case that I am kicking the tires of the parties' arguments, and therefore may ask questions that suggest I have a view that I don't in fact have. Answer only the question that is asked, please.

I do have questions for each side. If it turns out that you would like to answer a question that I have asked the other side that I did not think to ask you, I will give you that opportunity as well.

I want to just begin with two housekeeping matters. The first is, it did not strike me that the parties disagreed over the relevant standards for a motion to compel, a motion to suppress, or a motion to dismiss. So if and when I decide these motions, they will very likely be done by oral decision, and I probably won't spend a whole lot of time on the standards, assuming that the parties agree with them. If you don't, you will let me know. I appreciate there are very different views about certain cases on certain specific legal issues. But in terms of what one has to do to suppress evidence, or what is the standard for a motion to compel, I think there is agreement on that.

There is as well, and I can do this now or I can do this at the end -- I will do it at the end. There is a dispute over the trial date. Let's talk about that at the end because perhaps I will have greater clarity after I have heard the arguments.

All right. I begin then with questions regarding the motion to compel.

So, Mr. Klein, that is you, sir. You are welcome to stay where you are or go to the podium, as you see fit. I will just ask each of you, because I have had this happen, to bring the microphones closer to you because the acoustics in the courtroom are suspect. So let us deal with that.

Shall we begin, Mr. Klein?

MR. KLEIN: Yes, your Honor.

THE COURT: I will ask you to stand if you can.

MR. KLEIN: Sorry, your Honor.

THE COURT: My point was that you can stand here or stand at the podium. Whatever works for you.

MR. KLEIN: I will go over here.

THE COURT: Welcome to the podium, sir. Thank you.

Sir, I want to begin with the argument that you and your client need access to the communications regarding the MLATs in this case, and I believe in particular the one with the Netherlands. For me, there's a bit of a tension, or maybe there is just a gap between the argument that these MLAT communications are material to the preparation of the defense, and then the arguments for why, which to me are conditional, perhaps speculative, perhaps attenuated. I would have thought, and I do actually think, that there has to be some threshold showing beyond, these might be useful to us. And so I would like to talk to you about what that threshold showing should be.

Of course, you have offered some theories as to how there might be something useful there. I think that can be said in every case. I would think that there would have to be more than that. So let me please understand the showing that you believe you have made, and the showing that you believe you need to make, in order to obtain the underlying communications

regarding the MLATs.

MR. KLEIN: Yes, your Honor.

So, I think we would start with the standard we put in, that I don't think there is a disagreement on, with the *Stein* case and *Maniktala*——maybe I am mispronouncing that——but both indicate you need to have a strong indication that they might be helpful. So I will just start there. You don't have to definitively know precisely how they are going to help you, but you need to have a strong sense of it, and I think we do have that here.

We, of course, couch our language a little bit in the "may" or "might" because we haven't actually seen them and, I don't want to oversell to the Court, without having seen the documents, how exactly we may use them. But we know, generally speaking, and I was a former prosecutor, MLAT requests and the communications, again, can often involve substantive facts about the case. So they often include affidavits where an agent testifies, or in a form of a writing, to facts. They often include exhibits.

Now, having not actually seen them, it's hard to say, and the government didn't indicate exactly the nature of these MLAT requests or whether there are any communications where they have substantive discussions about evidence, about witnesses, about other things. So we are hampered a little bit there, but that's generally the case with a lot of discovery

requests, your Honor. And I think the case law indicates that's okay as long as we are communicating to you why we need these. And I think we were doing the best we could with some limited information.

But I would think, your Honor, if we look back and say, these are often like search warrant applications, or search warrant affidavits, which are provided to us on a regular basis in discovery. And, of course, the defense doesn't know before we get them what actually is in the affidavit, what it might say, why it might say it, are there exhibits attached, etc. So I think starting from that point, which is we need to have a strong indication or a strong sense of things, which I believe we do, and also what generally an MLAT request looks like.

Here, also I would say this case involves a lot of foreign evidence. So the government has produced to us what we understand, and we would like clarity, all the documents they received from the Dutch authorities. So from seeing those documents, we also know that they have requested things that are super-relevant to our case and our defense. So I would add that to the equation, your Honor.

THE COURT: I guess I am trying to understand what you mean by that. You have received foreign evidence from them. You therefore intuit, based on the evidence you have received, that what the government sought included materials that are

relevant to your defense. Why then do you need the communications with the Dutch authorities?

MR. KLEIN: Well, we don't need all communications, to be very clear.

So, if they are just e-mailing the Dutch authorities and saying, hey, can you speak on the phone today or when are we getting the MLAT requests, we are not asking for that. We are asking if there are substantive communications about substantive facts in this case.

THE COURT: Why would that matter?

MR. KLEIN: For example, they might have said, Can you give all of the things related to these, and they list five witnesses. And there might be witnesses we don't know about from other things, and the Dutch authorities didn't provide that because they don't have it, but the affidavit itself or the MLAT would contain that information. So that's an example I can think of off the top of my head. Or they might list categories of things they want, we want these seven things from you, and they got six, but one of those categories would be very informative to us in developing our case.

And, again, Judge Kaplan in *Stein*, it's not just like it has to be an actual exhibit that might come in trial. It would help us uncover admissible evidence. So I think that's one of our focuses here. We believe these would help us uncover admissible evidence.

THE COURT: Suffice it to say, I have years of experience with the *Stein* case, if you go back in the docket of that case. So thank you. I am familiar with it.

I understand the argument, I suppose. If they ask for seven categories of information and the government received six and there is not a category, what does that mean for you?

MR. KLEIN: I do think the witnesses is a better analogy here. If they say, give us all information on these five people, and they get information on four, and we haven't heard of the fifth person they're asking about, or they have communicated about that. Do you have information on this person? They have charged our client with a conspiracy here. So who they might think is involved in that conspiracy, they might not have been identified for us yet. So I am going to use that as the example.

THE COURT: All right. I understand that argument. I find perhaps less compelling the argument that you are somehow entitled to the government's theory of the case. I think there is some suggestion that perhaps these communications, and perhaps this is focused more on the communications with FinCEN and OFAC, but the suggestion that perhaps the government's theory has evolved, I don't know why you get that.

MR. KLEIN: Your Honor, that was one reason, and I will explain it in a little more detail because I used a shorthand in the motion. But that goes to the same idea. If

they are pursuing an avenue, Oh, we think this one avenue of evidence is relevant at this time, and later they no longer think that, maybe they have abandoned that theory because it's somehow helpful to our client. Now, I don't know what that is because I haven't seen it.

So, for example, they can say, Oh, we think how the alleged North Korean hackers performed this function and we want evidence on that. And then there is no evidence there. But that would actually be very helpful to us in rebutting the conspiracy charge that relates to the North Korean hackers, knowing that there was no evidence, that they couldn't find anything.

THE COURT: Let me think about that. There is a difference between pursuing an avenue of inquiry pre-indictment. Maybe you don't think so. If they are doing an investigation, not every tree is going to bear fruit. So the fact that there are some that don't bear fruit, I don't know if those inquiries were conducted before the indictment is issued. I am not sure why you get to see the evolution of their theory of the case.

MR. KLEIN: Well, the lack of fruit could be very relevant to us, proving that the actual tree has no fruit. So the lack of one --

THE COURT: You're not doing well with the metaphor extension.

MR. KLEIN: Again, our theory does not rest solely on this theory of the case. I will say this is a novel, complex case of first impression, so understanding their theory would be generally helpful to us.

THE COURT: You can't understand it from the really long speaking indictment?

MR. KLEIN: We did learn things also from their motion to dismiss opposition and other things. So I agree, we are getting a fuller picture of what they are saying. So I am not saying we are not. But again, our motion does not rest solely on the theory-of-the-case idea. And the cases that rejected it, one in which I was involved in, the *Hutchins* case in the Eastern District of Wisconsin, they are different and maybe would have relied more on that theory.

So, again, we have other grounds. I know you know the *Stein* case very well. If you look at the grounds Judge Kaplan laid out, we are also pinning our motion on other things, too.

THE COURT: Are you making an argument under *Kyles v. Whitley* that there is problem in the investigation of the case, that there was some sort of misconduct by the prosecution team? Because what you're saying to me sounds more that there are areas that you're not suggesting is being kept from you deliberately as much as accidentally, something that is not important to the government ends up being important to you. But I am asking, because there is a line of cases under *Kyles*

v. Whitley, whether you are making that argument, and if so, what showing do you have that there are flaws in the government's investigation that warrant disclosure?

MR. KLEIN: We are always mindful of that, your Honor. We are not making that right now. But, of course, we are keeping that in mind, and we are always on attention for those kind of things, but I am not resting this motion on that.

THE COURT: I appreciate you being so forthright about that.

Do you continue to believe that FinCEN and OFAC are part of the prosecution team? I saw that there were some changes in your reply brief or some modifications of your argument. So let me understand what today's argument is with respect to communications with those agencies.

MR. KLEIN: Can I just go back for one moment on the MLAT thing? I just want to make one more request, your Honor.

In looking at the cases the government cited, in at least one example the court conducted an in-camera review of the MLATs or the exhibits or whatever it was. We would make that request here. If you're not inclined to grant our motion, that at least you conduct an in-camera review of the MLAT request, the affidavits, whatever they have attached to it, and any substantive communications.

Now I will turn to the OFAC and FinCEN issue.

THE COURT: Thank you.

MR. KLEIN: We filed our motion based on the evidence we had or the information we had at the end. The government made a number of representations, which I walked through in our opposition, and it's on --

THE COURT: In your reply?

MR. KLEIN: Sorry. The reply.

So, because of that, we tailored our request.

THE COURT: Well, now it seems that you're asking for prudential *Brady* reviews. I am trying to figure out who is conducting those prudential *Brady* reviews, sir.

MR. KLEIN: We are asking for three things, but that is one thing we are asking for, your Honor.

THE COURT: Yes.

MR. KLEIN: So, we would ask that you order the government to order OFAC and FinCEN to do a prudential *Brady* review. I don't care who, whether it's OFAC or FinCEN or the prosecutors in this team, but someone conduct a *Brady* review of their files.

THE COURT: The concern I have, sir, is that my understanding for part of the reason of the development of the line of cases regarding who is in the prosecution team is precisely to prevent this from happening, where you can ask the government to go beyond the investigation it's done and to do the investigation you would like it to do. So there is a way in which it undermines those cases that define what the

prosecution team is. Let me try and say that a little bit more cogently.

If they were part of the prosecution team, of course, I can ask them to do all sorts of things, and the government would have an obligation. They are not, as I understand the case law. And because they are not, they are treated differently. So for you to ask me to order the government to do that prudential review seems to me to be an end run around an entire body of case law that is designed to prevent that.

You may say to me, Failla, it's really important, and I understand that. I have reversed convictions based on late disclosures of *Giglio* material. I am not averse to it. I don't want to do it again, but I will if I have to. I am just saying, we all can agree *Brady* is an important decision, the disclosure of exculpatory information is very important. I am not sure why I am out there ordering other agencies to do prudential *Brady* reviews.

MR. KLEIN: So, yes, it is very important, your Honor. I will start with that.

THE COURT: No one is disagreeing with that.

MR. KLEIN: The case law is a little more nuanced on that, I understand. Judge Rakoff, in *U.S. v. Gupta*, which is 848 F.Supp. 2d 491 (S.D.N.Y. 2012), my reading of that is Judge Rakoff didn't limit it, the *Brady* part, to just joint investigations, but also joint fact-gathering.

Now, I know the government has made a number of representations here that they have laid out all the ways they didn't work together, but there may be things beyond that. And that indicates that it's not so narrowly drawn. It's just a joint prosecution. So I think you do have room to order the government here to ask those agencies to do a *Brady* review.

We do have two other requests there.

THE COURT: Yes, sir.

MR. KLEIN: So, one is just to have the government confirm that they have produced everything they have received from OFAC and FinCEN. I believe that is the case, but it's not totally clear from my reading of their opposition. So we would like that confirmation.

THE COURT: Let me just ask this question though. Imagine a situation in which they make an overbroad request to FinCEN or OFAC and they receive material that is demonstrably outside of Rule 16 or *Brady* or Giglio. I think they would have the discretion to not turn that plainly irrelevant material over to you.

This may be a moot point if they have turned over everything.

MR. KLEIN: I am arguing against sort of myself here. If they have said they have turned over everything, or if they have said we have turned over everything, but we have withheld irrelevant things that don't qualify under any of those things,

then we will take that representation. But I just want to have some clarity on what they have done there.

The second, more minor sort of related request is because they have brought up --

THE COURT: Would this now be the third request?

MR. KLEIN: The third, subpart.

Again, we tried to narrow our requests based on the representations.

A case they put in was the *Griffith* case, which I also had in this district. The government made a lot of representations about not doing a joint review, and then later disclosed that the FBI actually, unbeknownst maybe to the prosecutors, had been contact with those agencies. So I would just ask that they confirm that their agents have not had separate contact with OFAC or FinCEN.

Again, in that case, we actually got substantive discovery that was very helpful to our defense because they had went and followed up. So we would just ask for that also.

THE COURT: Those were the questions I had regarding the motion to compel.

Let me ask my friends at the front table, is there a preference that we do each motion individually as distinguished from doing all the defense motions?

MR. ARAD: We would suggest, yes, your Honor.

THE COURT: Then I will hear from you.

There is something not fully satisfying about the retrospective nature of sort of the disclosure analysis. I am thinking in particular of cases like *Coppa*, which is the case we always cite regarding *Brady* disclosures after trial or after a guilty plea. And what you are supposed to do then is conduct this post hoc analysis of whether it would have been material.

I understand that. The problem with that is always that that supposes that at the end of the day the information will always come out. And I am a little bit concerned in light of recent, what I will call hiccups in this district, in cases like *Jain* and *Nejad*, that the government might, just by accident, by inadvertence, not produce everything that they are supposed to.

So, let me understand why you have such a philosophical opposition to turning over, for example, the MLAT communications. Let me just add to that, I thought the practice of the office was to turn over search warrant applications with Rule 16 discovery; is that correct?

MR. ARAD: That is correct, your Honor.

THE COURT: What is it about MLAT requests that make them so different from search warrant requests that they don't get turned over?

MR. ARAD: The difference, your Honor, is that MLAT requests involve diplomatic sensitivities that warrant applications do not. And so, from a policy perspective, there

are certain consequences that could flow from divulging those diplomatic communications that would not flow from divulging warrant applications.

THE COURT: Perhaps I can ask a better question, although I appreciate the answer you have just given.

I am just remembering MLAT requests that I have authorized and MLAT requests that I have prepared. There's some niceties in there. We thank you so much, and we give our highest compliments and all of that stuff. But I don't remember the actual application from the government being sort of beset with diplomatic issues. I appreciate what you're saying. Perhaps there are later exchanges about why there may be a problem or a concern about turning over information. That I get. But the actual application itself implicates these diplomatic sensitivities, and if so, how?

MR. ARAD: It can, your Honor. These applications often discuss the need for urgency with respect to certain applications, for example. That need can sometimes arise with the ways in which different governments interact with each other. That plainly is a diplomatic issue. That's just one example. But, as your Honor just noted, if we need to draw the line between the request and then subsequent communications, where at some point the diplomatic issues arise, that becomes a more difficult exercise.

Now, philosophically, this is the reason that MLAT

requests are different from warrant applications, but it is also probably more significant for the government's position on this issue that the law simply doesn't require that MLAT requests be disclosed. And the multitude of cases that are cited in our brief demonstrate exactly that. Certainly not where the defense hasn't given a concrete reason to believe that the MLAT request will reveal something that will be material to the defense. In fact, in the cases that the government cited in its brief here defendants made more of a showing than the defendant in this case has made. I will give just one example, your Honor.

I will wait for your Honor's cue on whether to dive into the case law.

THE COURT: I will let you. I do think you perhaps want to engage on the *Gupta* case, but perhaps you want to save that until our discussion about FinCEN and OFAC.

MR. ARAD: We can do that, your Honor.

The point with the MLAT requests here is that the defense's request is entirely speculative. It lays out a number of ways in which perhaps the MLAT request might be helpful. But any defendant could lay out all of those possibilities in any case, and that alone is not a reason to compel discovery of the MLATs.

THE COURT: Let me ask you that in a slightly different way, and you will excuse the analogy.

I have a couple of cases, additional to this one, involving classified information. And there is this concept of Section 2 meetings with the parties. And part of the reason for that is so that the parties can attune me to issues that I might not figure out are important to the case. They may be relevant to a government theory of the case. They may be relevant to a defense argument. But because I am simply not as steeped in the issue, I don't appreciate the significance until I am told what the significance is. So keep that as a concept.

A fear one could have is that the government might have a certain tunnel-vision in looking at materials and might not appreciate their significance or their materiality to a defense case. That is what I think Mr. Klein is suggesting to me. Could you help me understand why I should not be worried about that in this context?

MR. ARAD: At the outset, I will say that there is a risk that one could view something more narrowly than one ought to. But I think that that risk has been overstated by the defense in this case. The government, when reviewing documents and deciding what needs to be produced and what doesn't, takes an expansive view, particularly in light of recent hiccups that your Honor has described. So the risk exists, your Honor, but the presence of the risk doesn't necessitate an open-file discovery order on diplomatic communications.

THE COURT: One moment, please, sir.

Let's then talk about the OFAC and FinCEN communications. You have heard, and I took down if you didn't, Mr. Klein's three requests from the defense. I can ask them of you and you can tell me whether you wish to stave off or perhaps limit an issue by responding to them or you may tell me no as to everything. Do you recall what the three requests were?

MR. ARAD: I believe one of the requests, your Honor, was to confirm that the government has produced all of its documents that it received from OFAC and FinCEN.

THE COURT: Yes. Are you willing to speak to that issue or not?

MR. ARAD: I am willing to speak to it, your Honor.

I cannot confirm that the government has produced all of the documents that it has received from OFAC and FinCEN, but the government is not under any obligation to produce all of those documents. And I can confirm for the Court that the government has fully complied with its discovery obligations under Rule 16, *Brady* and its progeny.

THE COURT: Do you want to talk about the *Griffith* case request confirming, hopefully, that your agents have not had separate contacts of which you are unaware?

MR. ARAD: It's a little hard for me to confirm the negative. I am not aware of any --

THE COURT: I will try it this way.

Talk to your colleague and then get back to me.

MR. ARAD: We did speak with our agents, your Honor, in formulating our response to the motion to compel, and we can confirm that the FBI has not had outside contacts with OFAC and FinCEN. I believe that was the question.

THE COURT: It was. So no one is going to be surprised unless your agents are misremembering things, which one hopes is not the case.

MR. ARAD: That's right.

THE COURT: So that leaves us with this idea of the prudential *Brady* review. I have a little bit of skepticism of it. I have articulated that to the defense. But far be it for me to disagree with Judge Rakoff, but indeed, that is what I am doing. So if you want to engage with the *Gupta* decision or other cases in this regard, that would be helpful.

MR. ARAD: I think on the prudential *Brady* search there are a few points.

First, there just aren't indications that OFAC and FinCEN were part of the prosecution team in this case. They did not do the things that investigators do and that courts look to in deciding whether somebody is part of the prosecution team.

Second, I am not sure the government would be able to order OFAC and FinCEN to conduct a prudential *Brady* review. Regardless of whether it could --

THE COURT: Can I just hear that again?

MR. ARAD: I am not sure that the government would be able to order OFAC and FinCEN.

THE COURT: Of course. Could I? Yeah.

MR. ARAD: It's not for me to say.

THE COURT: It's always fun to be told you don't have the power to do something. If you think I don't?

MR. ARAD: No. I would not say so.

THE COURT: I would take that particular mantel from you. It wouldn't be your fault. It would be entirely mine.

I think the point -- again, going back to *Gupta*, perhaps what you're starting to say is that this case isn't Gupta. Yes, I am aware of that. But there are ideas in Judge Rakoff's decision that might be mapped on to this case, and that's what I want you to engage on.

MR. ARAD: It's difficult for me to see where the ideas in *Gupta* map on to this case, your Honor. One of the differences I think is that there is just no indication whatsoever here that the files that OFAC and FinCEN have contain *Brady* material. And so, we wouldn't even know what to ask them to look for if we told them that they needed to find *Brady* material. That would be a practical difficulty that we would face.

And in this case, where there are no such indications, I think it would set a dangerous precedent to require the

government to ask every third-party agency, with which it has any interaction in a case, to conduct a *Brady* review, without any indication that *Brady* exists there, without any indication of what exactly the *Brady* material would look like. If it were ordered in this case, I think perhaps it would have to be ordered in every case, and that would bring the government's investigations to a gridlock.

THE COURT: Okay. You're overstating the issue, but I get it. Thank you.

Are there questions that I asked of Mr. Klein that you wanted to follow up on that I didn't know to ask you?

MR. ARAD: No. Thank you, your Honor.

THE COURT: Thank you.

Mr. Klein, brief reply.

MR. KLEIN: Yes, your Honor.

We would be fine in the first instance of taking the MLATs that removes the diplomatic niceties that the prosecutor mentioned are one of the reasons for not handing them over. I also remember doing MLAT requests, and I remember them being much like your Honor does. So we are fine if they want to remove some of this diplomatic language or whatever it is that causes this concern and have a redacted version that is more focused. So I will start there.

Number two, when the prosecutor mentioned there is no indication that OFAC might have anything that's *Brady*, that's

just not true, your Honor, in my opinion. They produced to us a report from OFAC that is 60, 70 pages long, it has over 200 exhibits, on Tornado Cash, on what happened here. So there is a strong indication that OFAC has done a thorough investigation about this and may have materials that are *Brady*.

So, the one thing we received from the government was this report. We have recently asked them to provide us an unredacted version and the exhibits; they haven't responded yet. We hope we don't have to come back to your Honor on that issue. But there is an indication that they have substantive materials and have done a substantive investigation and therefore could have *Brady* materials.

THE COURT: Thank you.

Let's move, please, to the motion to suppress. Is that Ms. Axel?

MS. AXEL: Yes, your Honor.

THE COURT: Understand that my first question to you comes from the perspective of a very busy district judge.

Given that the government has had no success in opening up any crypto wallets of any type, is this even something about which we should be concerned?

MS. AXEL: Yes, your Honor, and we did anticipate that question. I think we appreciate, too, I don't think the government here takes the position that the issue is not ripe. They didn't in their papers. They didn't in our

meet-and-confer on the issue.

Your Honor, we think there are obviously important fundamental rights here, including defendant's Fourth Amendment right that would be abridged if the government were to continue to try to use these devices to go off on to the internet and try to seize assets.

THE COURT: Just to the point you're now raising. Imagine counter-factually that the government goes to some judge somewhere next week, I won't say tomorrow, and gets a search warrant or a seizure warrant for, for example, the hardware wallets or the devices on which information about the wallets is held. Does that alleviate any of the concerns that you have expressed in your suppression motion?

For example, one of the things that you're saying is that the warrant is an inappropriate seizure warrant. Something else is that there is a question about things being in the residence or not being in the residence. And I thought one of the points that you had was that the government is sort of telescoping its search warrants by allowing or arrogating for itself the ability to search not merely the things -- well, to search the things it has found as a result of the search. And for that latter argument, I suppose, and I am just thinking, and I will talk to the government about this too, I am thinking about situations where the government conducts a search and finds phones or laptops. I thought the practice, or

at least it had been at one point, was to then get a search warrant for the individual devices, and not to use the search warrant that you used for the residence or for the business to then search the computers.

Go ahead.

MS. AXEL: I want to make sure, backing up a second, that we are still not confused about what our position is.

THE COURT: Let me hear it then, please.

MS. AXEL: Our position is not that they cannot search the devices. They don't need a separate warrant to search the devices. That is not our position. They can open the wallets. They can search the so-called wallets. I would return the Court to maybe reverting back to our reply on this, because I think we swatted away those hypothetical sort of histrionic arguments about us asking for limitations, in the government's brief.

THE COURT: I didn't think you were calling me histrionic. I am not sure their arguments rose to that level, but go ahead.

MS. AXEL: Fair enough, your Honor. But there were some sort of worst-case scenario things that we are trying constrain the government's ability to search devices it seizes on the property, and why were we not making that same argument with respect to the laptops or the phones? And what we said is, our position is the same with respect to these little USB

devices, and, in fact——and we may get to this in our argument——sometimes now these wallets actually look like an ATM card. So whether it looks like a USB device or an ATM card, or whether it looks like a phone or a laptop, our position there is I think consistent with settled law here. If those devices are on the premises, they can search those devices.

THE COURT: Of course.

MS. AXEL: So I think the distinction here is that, if they want to go out on the internet and then seize cryptocurrency, or if they want to use an ATM card or passwords found in a defendant's residence to go seize assets in his bank account, they need a separate warrant for that. That's a really important procedural safeguard, your Honor.

First of all, if they had tried to actually prepare this warrant under the venue provision that they have cited, in order to go out on the internet and get something, they would have had to make a much more particularized showing. This is totally overbroad with respect to any and all cryptocurrency. And we see this, your Honor, not just in this case, but we do see this in cases across the country, where they are sticking this language in this --

THE COURT: Which language is "this language," please?

MS. AXEL: The language in Ms. Hutchins' affidavit that says that cryptocurrency is found on the wallets. And that's misleading. No personal animosity towards Ms. Hutchins.

I think this is a government policy that they include this language.

And then we see the sloppiness that happens then, and we see it in the opposition brief. On the one hand, the government admits that actually cryptocurrency lives on the internet; it lives on the blockchain. It does not live on these wallets.

THE COURT: What district are we then submitting this? As a practical matter, if it's on the blockchain, to which judge is this warrant being directed?

MS. AXEL: I think Rule 41, the subdivision they have provided, absolutely provides for them to be able to get a warrant for that. In fact, we have a string cite in the reply brief where we show that the government knows exactly how to do this. We have cited multiple cases. I can direct the Court to it.

At footnote 4, the case in the text --

THE COURT: What page, please?

MS. AXEL: Page 7, footnote 4.

First, the *Firoz Patel* case is a criminal warrant in a criminal case in the District of D C. Then the four cases in the footnote are civil seizure warrants. But there is no issue that once the government has the passwords and has the tracing on the blockchain, they can come to a court and ask a magistrate to issue a particularized warrant to seize those

assets.

But that's not what we have here. We have a premises warrant to go into Mr. Storm's home. And with that warrant they can only search and seize what is in the curtilage of that home, and only for evidentiary purposes.

THE COURT: Again, to my hypo, if they went next week to get warrants of the type that are described in footnote 4, or on page 7 of your reply, are you suggesting or arguing to me that it is too late in the day for them to do that?

MR. AXEL: No.

THE COURT: I ask because you cite the *Kyllo* case and there is a suggestion, which I understand, that if the government obtains something by improper means, there are certain times they can't fix it. I did not understand, if that case was cited, to make the argument that it can't be fixed here. Your suggestion instead is that, rather than rely on the warrant for the residence, they should have appropriate, particularized warrants for this information.

MS. AXEL: I appreciate the question, your Honor. That occurred to me as well when I reread the brief in anticipation of this argument.

Your Honor, I think it would violate the warrant to go out on the internet and use those passwords that it obtained through this search. It would go beyond the scope of the Fourth Amendment. I am not saying we wouldn't then move to

suppress that evidence, because using the passwords they went out on the internet. But obtaining the passwords themselves, we would not argue is a violation of the Fourth Amendment because the passwords are on the devices in the home.

THE COURT: So, potentially, there is a needle they could thread. But, potentially, your argument would be a fruits argument, that they could not now, having done what they have done, go and obtain warrants for the wallets and other devices. This I understand. Thank you.

MS. AXEL: Yes.

THE COURT: You will take this the right way. I found less compelling what I think was your last argument, which was the suggestion that this was an end run around the asset forfeiture laws. I thought the government explained that that was another process. But let me understand your current view as to the interplay, if any, between your motion to suppress and the provisions for civil and criminal asset forfeiture.

MS. AXEL: Your Honor, I do think there is an important distinction between a search warrant and a seizure warrant. And I also was an AUSA and I dealt extensively --

THE COURT: Everybody other than Mr. Patton is going to be able to say that.

MS. AXEL: I dealt extensively with foreign forfeiture warrants in a case where I think, your Honor, there were assets all over the world. And I have a heightened sensitivity to the

type of tracing that is required to go seize assets for forfeiture purposes. And it's also very clear in a forfeiture context, your Honor, that you can't seize substitute assets pretrial.

So, because of that, I think, the tracing in a forfeiture warrant is very clean and focused, and this "any and all cryptocurrency," when obviously someone like Mr. Storm has other, outside of the Tornado Cash protocol, has other cryptocurrency-related projects, in other words, your Honor, he has money that even the government would concede is clean. And so having this "any and all cryptocurrency" connected to wallets in his home, there is a breadth that happens in a search warrant of someone's home that doesn't happen in a seizure warrant. You cannot have substitute assets.

So I think if we are very clear about this process, the search warrant allows for seizures for evidentiary purposes. If it so happens that then you can then under criminal forfeiture statutes seize that property, then so be it. Then that may be appropriate. But you still have to satisfy first of all the search warrant standard. And if you don't have it, you really should get a seizure warrant, and there would be heightened standard for the type of tracing requirement.

THE COURT: I am not disagreeing with what you are saying. I guess I understood the government to be suggesting

that part of the reason it seeks to seek this cryptocurrency is not for asset forfeiture purposes, although they do make some noise about this being the proceeds of some of the conduct, but I thought as well that it had, in their estimation, evidentiary purposes. And to that end, they were having difficulty disentangling what portion of the crypto was, in fact, traceable to original TORN tokens, which a portion of which was traceable to something else. So I thought that was part of the reason as well that what they were seizing had less specificity than you might like.

So, what I am saying is, I am putting now to the side the asset forfeiture issue. To the extent that they are seizing this for evidentiary purposes, and to the extent that they tell me they can't disentangle what is and is not relevant evidence, why can't they seize it while they figure it out?

MS. AXEL: Your Honor, I think that's clearly overbroad.

Again, let's go back to the bank account analogy. And even the government uses this. But there is no reason why bank accounts are different than crypto accounts, other than we are all very familiar with them. There is a statement in the opposition, something like, the government, of course, would never go out and try to seize a defendant's entire bank accounts because there might be some assets that were tainted on them.

And that's the case. No magistrate in this courthouse is going to grant that. If you come in and say, the defendant has some money that's tainted in his bank account and we can't trace it, because perhaps there is foreign evidence or some reason why we can't figure out which of -- he has 10 million in his bank account, 2.6 million is tainted, and we want to seize it all for evidentiary purposes under a search warrant. No magistrate in this courthouse is going to grant that.

So, that's the standard here, your Honor. That would violate the particularity requirement of the warrant. They have to actually show for evidentiary purposes what specific -- they have to have better tracing for the criminal purpose, the probable cause and the criminal purpose, and the actual moneys to be seized. And I think that that standard would be very clear if we were really looking at a warrant that went to his bank account. But I think that that's a fair analogy.

THE COURT: Thank you very much. Unless there is anything you need me to know that I have not asked you about.

MS. AXEL: No. Thank you, your Honor.

One thing, I guess. You did ask me about remedies.

So, I would say that, having thought about this in anticipation of the argument, what we would simply ask the Court to do is to use its power to excise both the words "any and all" in paragraph 16 and to strike paragraph 17 of the

items to be seized. And that would affect the remedy that we are seeking.

THE COURT: Thank you very much.

Mr. Gianforti.

MR. GIANFORTI: Where would you like me to start, your Honor?

THE COURT: As you can tell from my first question to Ms. Axel, I am trying to limit this or short-circuit this as much as possible. Why can't you get a supplemental or a second warrant, as they have suggested in their papers?

MR. GIANFORTI: We could. We certainly could. The issue that we face, your Honor, and it wasn't raised squarely in our opposition, but I think it's certainly implied in some of the things we said, I think this is completely unripe at this point. We have seized nothing. We are talking about suppressing evidence that we don't have. We are attempting to access these wallets.

THE COURT: Let me make sure I understand because I thought I saw in your opposition that there were items that you seized that might have, for example, what I know to be private keys or information of that type.

So you have told me there is a hardware wallet. What does that look like? Does it look like a bank card?

MR. GIANFORTI: I believe it looks like a USB. I haven't physically seen it. It's some kind of hardware device

that contains the private keys.

You are quite right, your Honor, that some of the evidence that was seized from his home was, I think, scraps of paper that appeared to have private keys. We haven't been able to connect up those private keys to any particular wallets on the blockchain such that we may try to seize cryptocurrency. If we were to determine, say, that that private key led to a wallet that had cryptocurrency that was traceable to the offenses, we would seek a proper seizure warrant, not the sort of search and seizure warrant we have here, which was meant to seize evidence. As we have laid out in our warrant and in our brief, cryptocurrency here could form evidence of the charged crimes, at least $2.6 million of the cryptocurrency that Mr. Storm had represents the proceeds from the Tornado Cash scheme.

THE COURT: Let me understand what you think you have seized. You do have a warrant application and a warrant that you believe allows you to search for and seize any and all cryptocurrency, correct?

MR. GIANFORTI: Correct.

THE COURT: Right now today you didn't actually seize any cryptocurrency; also correct?

MR. GIANFORTI: Correct.

THE COURT: Why——and I am not telling you to do something, I am asking a question——why not agree to excise that

portion of paragraph 16 and strike paragraph 17? Because you don't have any right now. At most, what you have is information that might lead you to find cryptocurrency or wallets somewhere down the line, at which point you were starting to tell me you might then ask for another warrant. I am actually trying to understand what the gap is between the parties, and I am sure you have discussed this in meet-and-confers that I wasn't present at, so maybe you both know this. But you today don't have cryptocurrency.

MR. GIANFORTI: That's correct.

THE COURT: Maybe some day you may be able to find it with the information you did seize, in the same way it would be like going to a home and getting a bank account statement and being able to thereafter subpoena information about the account and perhaps seize funds from the account.

So, I guess I am trying to figure out, having now heard me speak at some length with Ms. Axel, what is the difference between the parties on the issue of the request in the warrant for the seizure of cryptocurrency?

MR. GIANFORTI: I don't think there is one. Because I think we are on the same page in terms of what a search warrant like the one we got allows and what a seizure warrant for forfeiture purposes allows. And we readily admit that what we got was a search warrant which allows seizure for the preservation of evidence. And these devices that we are

attempting to get into, we may get into them before trial, at which point we may be able to link up particular cryptocurrency to the crimes that are charged, at which time we would seek a subsequent seizure warrant.

THE COURT: Well, perhaps, then, Ms. Axel may come back to me and say that the Fourth Amendment damage has already been done by obtaining information that allows you to examine what you did seize, the scraps of paper with private keys and things of that nature.

I realize I sound as though I am talking out of both sides of my mouth. I promise you I am not. I am really trying to understand the issue.

The defense has said to me that they are fine with you obtaining certain materials during the search, that there were things that you could properly seek during the execution of the search warrant. They are concerned about you going off and trying to get things off of the internet. And they believe that what you should do is to have a more particularized warrant with respect to the crypto assets. And you're not disagreeing with them as much as you're saying, we haven't been able to get any cryptocurrency just yet, and maybe some day we will, and maybe some day we will issue a second warrant. So that's why I am trying to figure out what the difference is between the parties.

To that point as well, I began by asking Ms. Axel

whether this was ripe, and she said yes, because it's not as though you have stopped looking at what you have seized. You're telling me it is not ripe, and I wanted to understand that better. So excuse the extremely compound question.

MR. GIANFORTI: I think I see where you're going.

So, maybe this will be helpful and you can tell me if it's not. We use this example in our brief. This is really no different than when the government goes in, as we did with this warrant, and seizes a bunch of electronic devices, like phones and laptops, and is able to bypass their encryption or whatever, and then does a responsiveness review. So we get into a phone, we look for evidence of a crime, and that's the evidence that we then have, and then the rest of the evidence we don't use because it's not responsive to the warrant. This is the same thing where we are going into --

THE COURT: One moment, please.

And this is where my information may be dated. You have a warrant that permits you to search for and seize electronic devices. But I thought you then needed a separate warrant to open the devices. You're saying that's now telescoped. To the extent that you find a laptop, you're authorized to open that laptop -- okay.

MR. GIANFORTI: The warrant covers both. Every premises warrant that I have executed in the job covers both the search of the house for items and then the access to those

items.

THE COURT: I understand that.

You may continue. Thank you.

MR. GIANFORTI: So, your Honor, if we get into these devices, as we would any phone, we will look at them, we -- I think what sounds like the concern here is that we are doing some kind of an end run around the forfeiture process and attempting to drain this man of all of his wealth via a search warrant, which is not at all what we are trying to do. We are trying to simply access these devices, that may point us in the direction of cryptocurrency that is evidence and proceeds of the crime. If that cryptocurrency ends up being forfeitable, it will be subject to the forfeiture process in connection with this case.

THE COURT: I think there is a second issue that Ms. Axel was raising, and that is, the use of the term "all cryptocurrency" suggests or may suggest a measure of overbreadth because you don't know today how much cryptocurrency Mr. Storm has. You might imagine that not every token, every bit of it he has, is either evidentiary to prove the government's claims in this case or that it's subject to asset forfeiture. And, as Ms. Axel noted, you can't seize substitute assets.

So there is a question about whether the manner in which you have sought to locate this cryptocurrency is itself

overbroad because there hasn't been a sufficient particularity. For example, you didn't say, I would like to seize that cryptocurrency which appeared on the wallet after the OFAC sanctions were imposed because I am confident, or at least I have probable cause to believe that that is traceable to the offense, as distinguished from the stuff he has accrued over the preceding several years.

MR. GIANFORTI: The trouble, your Honor, is the way that cryptocurrency exists. Once we get into it, it's sort of this undifferentiated mass, and then we have to use tracing analysis to determine what portion of it is evidence or fruits of the crime.

So we would theoretically get into a wallet. Let's say we get into a wallet and it indicates that that wallet contains -- TORN is actually kind of a tricky example. I think we would say that any TORN is sort of evidence of proceeds of the crime. Let's say we were to get into a wallet and it contains ETH, or one of these stable coins which is linked to the US dollar, which is a common thing that people convert cryptocurrency into. We need to get access to that wallet in order to do the tracing analysis that shows that it is linked to the crime in some way.

So that's the issue. It's a little different than, say, a bank account. First of all, you don't search a bank account. You can submit a subpoena, as you well know. And if

we have reason to believe that a million dollars of the crime proceeds flowed into an account, we can do that tracing analysis through subpoenas and the like and figure out whether it stems from a particular crime and then we go and seize that million dollars from that account.

With cryptocurrency we go in and say, okay, we have got 100 ETH sitting in this wallet. That doesn't tell you anything. So then we have our really smart tracing people look at it and they say, well, this ten ETH came from this transaction on the blockchain; and if you go back far enough this represents, this would be the TORN tokens. So we are then able to determine what is seizable from that point forward.

So, again, it's a little bit like the phone, when you go in you don't know what you're going to find, and only by going through it and looking at it are you able to determine what is actually evidence responsive to the warrant. It's the same thing here.

THE COURT: Those are the questions I had for you. Are there responses you had to questions I asked Ms. Axel?

MR. GIANFORTI: I don't think so, your Honor. Thank you.

THE COURT: Thank you.

Ms. Axel, do you want to be heard in reply?

MS. AXEL: Just a couple of small things, your Honor.

THE COURT: Is there no gap that can be bridged here?

You have now heard me have different discussions with Mr. Gianforti. Is there anything, based on my conversation with him, that might lead you to believe that a further meet-and-confer might clarify the parties' positions?

MS. AXEL: It's somewhat puzzling, your Honor. Actually, on the one hand, the representation that they might be willing to go get seizure warrants would close the gap. But I think the gap closer, your Honor, is the remedy that we proposed.

Mr. Gianforti said, they open the wallet, they see 100 ETH on the wallet. There is no ETH on the wallet. It's just passcodes that tell you what you can access with that wallet. It's like your ATM card, going back to our factual analogy. But the rest of what he said I agree with. Once they open it and they see the passcodes, they can map the crypto, they can see where it came from, they can see what it went to, and then they can take the next step of getting authority to go seize something.

THE COURT: Based on what you understand the government to be doing right now with the information it obtained from the execution of the search warrant at Mr. Storm's residence, you have just heard Mr. Gianforti tell me what they are doing, and what they had success with and what they have not had success with. What of that is violative of the Fourth Amendment?

MS. AXEL: Your Honor, accessing the devices is not violative. But, they have not taken off the table seizing any and all cryptocurrency.

So, our remedy is, if you look at paragraph 16 of the warrant, it says, Any and all cryptocurrency, to include A, B, and C. We are actually okay with A, B, and C. It's just the "any and all cryptocurrency" that's the problem. But A, B, and C is what is on the wallet, which is: Representations of cryptocurrency public keys and addresses; representations of crypto private keys; any and all representations of cryptocurrency wallets or their constitutive parts to include seed phrases and recovery seeds. We would be okay with that. That allows them to search the devices.

THE COURT: And if using the items that are listed in A, B, and C they find something, then they come to me or someone else to obtain a warrant to seize?

MS. AXEL: That's why we also need 17 excised, because that's the real problem.

17 says, The United States is authorized to seize any and all cryptocurrency by transferring the full account balance to a public cryptocurrency address controlled by the United States. That is the big problem. So that they should not be permitted to do.

THE COURT: Stay there, please.

Mr. Gianforti, is there not a tension between having

paragraph 17, which seems to allow you to seize the crypto and move it somewhere, and telling me today that you would be seeking a second warrant? Could I understand the reconciliation of that?

MR. GIANFORTI: Your Honor, as I said before, this warrant is really about securing evidence, and to the extent any and all cryptocurrency is evidence of these crimes, we would move it to an address that we control for the purposes of evidence preservation. If we were intending to then forfeit that as the proceeds of a crime, we would follow it up with a seizure warrant.

THE COURT: Thank you. And I will let Ms. Axel continue based on that clarification.

MS. AXEL: And now we have our clear Fourth Amendment problem. Because they are using passcodes, like taking your passwords that are next to your desk, or taking your ATM card that they seize from the drawer, and they are going to the bank and they are using that information to now seize your assets. For whatever purposes, that is beyond the curtilage of the home. That is using information found in the searched premises to go seize assets that were not in the searched premises.

That's the point, your Honor.

THE COURT: Are there any other points you want me to know?

MS. AXEL: I think that is the key problem that we

have here, your Honor. It's the using information found in a searched premises, one that one does have probable cause and a warrant to search, and to go out on the internet or to some other place. I think the Fourth Amendment clearly does not permit that. You need a separate new warrant for that.

THE COURT: Mr. Gianforti, do you agree or disagree?

MR. GIANFORTI: I find this curtilage argument a little puzzling, if I can borrow a word. On the one hand they are saying go out and get a seizure warrant. On the other hand they're saying you can't seize crypto because it's outside the home. That doesn't make any sense. Under that argument, because cryptocurrency resides effectively nowhere, we would never be able to seize cryptocurrency. That's the logical conclusion of their argument.

Again, I think this word "seize" that appears here, I just can't help but think the defense is seeing the word seize as though it means forfeiture. It's not forfeiture. This is securing evidence. And if we want to move forward and forfeit that evidence because we think it's the proceeds of a crime, we will do so appropriately under the forfeiture law.

THE COURT: Everyone is done on the suppression points?

MS. AXEL: Yes, your Honor.

THE COURT: Thank you.

I am ready to go forward with the motion to dismiss,

but just in deference to our court reporter, and given the fact I think that will be a longer argument, perhaps we will take a five-minute break. Is that acceptable to everyone?

MR. REHN: Yes, your Honor.

THE COURT: I will see you then. Thank you.

(Recess)

THE COURT: Mr. Klein, perhaps I can begin with you, sir, on the motions to dismiss. And this is a general question, and I understand completely if you want to defer to someone else on your team. But one of the questions I had was that I felt in reading the parties' submissions that you were almost talking past each other at times. There is a narrative that you have given to me and there are themes to your submissions. And yours is, this is software, this is the criminalization of thought. He just built a better mousetrap and he is now being prosecuted for it. And then on the government's side, there is a lot of no, no, no, this software is only one component of what it is that they are prosecuting him for. It is beyond just putting Tornado Cash out there. There's more acts.

My question, sir, and I will actually get to it, is, I question my ability to decide among the factual narratives that are being presented to me in the motion papers. I feel almost like I am stuck with the pleading language in the indictment, especially on the issue of intent. And if it turns out the

government can't prove that, your client gets acquitted. But I am not sure I get to dismiss the case based on what you say is the narrative of the case, when the government says that is not, in fact, what we are alleging. So help me understand how I have the power to basically kill it before it grows, and to let this case be dismissed without allowing a jury to even consider the government's evidence and allegations.

MR. KLEIN: Yes, your Honor, and we think it is important that you kill it before it grows.

So, I think we did put in some factual narrative about Mr. Storm, his background, some things that are beyond the scope of the indictment, just so your Honor can get a sense of who our client is and some of the background. But I think on key points that would allow your Honor to dismiss this case on all three counts, there's not disputes, and their factual allegations, read by them, by us, and the Court, would permit that.

So, you clearly have grounds under Rule 12 to do so. And Rule 7, which you can look to about a properly formed indictment, doesn't still override Rule 12, they have to state an offense.

So, their factual allegations do not state an offense, and we lay out those reasons. And there's key undisputed points, and I will give a few on the part I am talking about, the 1960: The lack of control, the immutability. Those two

key points right there, which they don't dispute; they dispute the legal significance of them, but they don't dispute those factual allegations.

THE COURT: On the immutability point, I thought what they were saying was that all that was immutable was the operation of the pools. And you refer to it as the protocols. You each refer to it differently. I want to make sure you're talking about the same thing.

MR. KLEIN: Yes, your Honor. We are talking about what was immutable was the pools.

THE COURT: And then the lack of control. But please continue, sir.

MR. KLEIN: So I think your Honor is on safe ground. And it's actually very important in a case like this, where they are advancing a novel complex theory, really a first impression——the 1960, my colleagues can speak on the other parts——that my client should not have to bear the burden, expense, stress, go all the way to trial and then on Rule 29 we win. So I think it is important that courts do dismiss cases -- I agree it's rare, but they do dismiss cases when things are like this.

Now, we don't dispute their indictment is 36 pages.

THE COURT: Yes. It is what it is. But they do accurately recite the statutory language, do they not?

MR. KLEIN: Yes, they do, your Honor.

THE COURT: So they are fine on Rule 7 purposes. They are adhering to the statute, and they are giving you a sense of what it is they believe your client did that is violative. You just believe that what they have stated does not suffice.

MR. KLEIN: Yes, your Honor, that's the basis of our motion. Each count has different failings that are fatal to it, and there are different factual allegations that are undisputed that lead there. But, yes, that's exactly our point.

THE COURT: You have mentioned the immutability argument so perhaps I will talk to you about that now.

The government suggests that independent of the operation of the pools, that there were aspects of Tornado Cash that Mr. Storm or his colleagues retained the ability to affect or to control. Do you agree with that?

I am not sure that they told me what all of them were, but to them immutability means less than what it means to you. So I would like to understand why immutability, why you believe it is dispositive, because you suggest that it is, and whether you and the government have completely coextensive use -- let's perhaps close the door.

So I guess I would like, perhaps, if I can have the CliffsNotes version. I understand what you believe to be immutable. I want to understand better its significance. Thank you.

For example, sir, is it because the immutability predated the charges in the case, is it because it impacts in some way your client's ability to form the requisite intent, or something else?

MR. KLEIN: Yes, your Honor. It is relevant for a number of reasons. I will focus on 1960, your Honor, because that is what I am going to talk about, and Ms. Axel can talk about the other two counts in particular.

For 1960, the pools, which are immutable as of May 2020, predates their time period they are looking at, because they are immutable, our client had no control, or no one had any control, other than the user, over the cryptocurrency. And that goes to the core of 1960.

So when it's immutable, it's a software that's running, it's open source, it's immutable, and it's noncustodial. So there are other elements there. The immutability is part of that.

So our client had no control, and that's why we emphasize that repeatedly throughout our motion and our reply, that those provisions of 1960 and 1960 itself, to be a money transmitter, control is key. It's one of the key limiting principles of that statute. And it's what distinguishes a software provider from, like, a software service provider.

The other components that your Honor is focusing on, like the UI, so I will take the pools as one and the UI as

another.

THE COURT: And I guess the relayer network.

MR. KLEIN: Yes.

So the pools are on chain. And some of the amicus talk about this too, your Honor. The pools are on chain. The UI is off-chain. And the UI is just a way to access the pools. But the UI itself does not give my client any control or anyone else, other than the user, control of the funds that are transmitted. It's just a way to interface. It's just a nicer way to interact with the pools. You could still do everything you need to do without using the UI. And we believe, and they don't allege differently, for example, that the alleged North Koreans didn't even use the UI.

So the UI is a component that is not necessary, not required, and simply is a way to, like, in a nicer package, interact with the pools themselves. And the pools themselves are why Tornado Cash exists. That is the important component. And again, those were open source, noncustodial, immutable.

So that goes to the control on it, which is super key for 1960.

And the pools -- again, my client didn't control them.

Does that help answer the question, your Honor?

THE COURT: With respect to 1960.

Am I mistaken in thinking that you're suggesting immutability goes to intent?

MR. KLEIN: Yes, it does. And I believe we briefed this issue on the sanctions and other parts of it.

THE COURT: So you're deferring that to your colleague.

MR. KLEIN: Yes.

THE COURT: You are then the person I should be talking to about money transmitting businesses, what they are and what they are not. Could you speak to the government's argument that they have alleged in the disjunctive that -- and they have adequately alleged a transaction that in any way or degree affects interstate or foreign commerce?

MR. KLEIN: Your Honor, I believe that's in the money laundering section too. Ms. Axel will address that question.

THE COURT: Then you and I are going to run out of questions pretty soon.

MR. KLEIN: I am fine with that, your Honor.

THE COURT: That's fine.

Mr. Klein, are you speaking to overbreadth or is that also Ms. Axel?

MR. KLEIN: It's actually Ms. Axel or Mr. Casey.

THE COURT: Sir, I don't have additional questions for you, but I'm sure there is something you want me to know, so go ahead.

MR. KLEIN: Your Honor, I would really emphasize for you the importance of looking at the lack of control, the lack

of a fee, and then the express exemption for network access or a software provider.

THE COURT: You do speak of lack of fee. The government responds by saying that in fact there were fees. They may have been a little bit more circuitous than you are suggesting, but it's not as though your client was doing this out of the goodness of his heart. He was earning money for this.

MR. KLEIN: So my client, there is no allegation he ever received a fee, to be very clear. Their only allegation is that some relayers might have charged fees for some transactions.

THE COURT: I thought that they structured the network of relayers in a way that they thought was useful to them.

MR. KLEIN: All they did, your Honor, there was a vote on the protocol that set up a network of relayers based on how many TORN tokens they had. And on the UI, all it did was have a list of optional relayers. That was it.

Again, it was just a way for someone to quickly look at something; it was a provision of information. They didn't charge a fee when you picked a relayer. They didn't get a fee from that relayer. That's it.

THE COURT: All right.

Anything else you would like me to know?

MR. KLEIN: No. I just think that the real important

thing is the software component here is providing the software versus providing a service. And I think the limiting principles that are really important here is to focus on the lack of control, which is implicit throughout 1960, as well as the fee, which my client did not charge. The UI did not charge a fee, just to be very clear.

THE COURT: As you tell me each thing, you're actually implicating questions, which is great.

This software service dichotomy that you're saying to me is something the government, again, opposes mightily. They suggest that it is the functional capabilities of Tornado Cash and not some abstract software in the ether that matters. Is that for you to speak to or one of your colleagues?

MR. KLEIN: I can speak to that. I think what is at issue is all software, to be clear. Every component is software. So there are different components. My client had involvement in levels involving each component.

THE COURT: Perhaps I can ask a better question, so let me do that.

If your client created Tornado Cash and just put it out there and never did anything with it again, I am not sure we would be here today. What I am understanding the government to say is that it is not merely that your client developed and implemented Tornado Cash, but that he remained involved in its operation, and actually did things with it. So I don't think

he is being punished for having been a good software engineer. I think the point is that it is what he did with it, particularly upon receiving notice that there were incidents of fraud or hacking or sanctions. That's why we are here. That's what I understood.

So I am reacting, and sort of bristling a bit, at your suggestion this is all about software, because the government keeps telling me it's not. A jury may decide that that's all he did, but they are vehemently opposing that argument. So I do need you to sort of engage with the government on what they think the conduct is. And that goes back to my first question to you, sir, in this section.

MR. KLEIN: Your Honor, again, I think the key thing here is that that really speaks to a negligence standard. You could have done more, you learned something and you could have done more. Which is not our standard here. For 1960, there is not an intent element. It's essentially a strict liability offense. If you're a money transmitter and you qualify, then you're guilty. And our argument is, he is not a money transmitter. Maybe the points you're raising, there might be some other criminal statute that covers that part, but definitely not 1960, for the reasons I have articulated. So I think that is the key point.

THE COURT: Thank you very much.

This time I think I would prefer to hear from the

individual defense attorneys, and then I think it's Mr. Rehn who is handling the motion to dismiss and I will ask all my questions at once.

Welcome back, Ms. Axel.

Ms. Axel, if your focus is on money laundering, then that's where my focus will be as well. And I hate when people ask me hypotheticals, but I am going to ask you a hypothetical.

If there is an individual who runs a concededly legitimate business, a restaurant, and someone approaches that individual and says, I would love to use your restaurant bank accounts to deposit the proceeds of criminal activity, because then I can deposit them and it will be laundered and no one will know where it comes from, and you will make something for your efforts. That suggests to me, if the restaurant owner knowingly, intentionally gets involved in this knowing that it is the proceeds of some unlawful activity, there is concealment of money laundering.

So, I ask that because there has been a focus here on the fact that there are legitimate aspects to Tornado Cash and that not every client was a felon in training. So saying, for example, that your clients did not have agreements with the perpetrators of the underlying unlawful acts, well, your client didn't need to engage in the underlying acts so long as he understood, potentially, that Tornado Cash was being used to launder those funds.

So my point is, I am trying to understand how the traditional money laundering model can be transferred, if at all, to the Tornado Cash or to the cyber setting.

Separately, I didn't want you to focus too much on your client's knowledge of or involvement in the underlying criminal acts as much as his knowledge that the proceeds of those criminal acts were being laundered through Tornado Cash.

So, can you help me with those things?

MS. AXEL: Yes, your Honor. And, yes, we are all nervous of hypotheticals in this particular context, but the hypothetical there your Honor gave us is very clear, a person that actually conducted the financial transaction knowing that the proceeds came from some form of proceeds of SUA.

So, there, your Honor, I think that is the paradigmatic kind of example you have in drug conspiracy type cases or car wash cases, where you have someone who agrees, knowing that the proceeds come from some illegal activity, to wash them through the process.

And, your Honor, what I would like to submit, it's sometimes difficult to prove a negative, but what I would like to submit to the Court is, having looked at every single conspiracy case they have cited and that we have cited, there are none where you either don't have the defendant being actually a participant in the conspiracy to the substantive offense. Of course your Honor sees that all the time, drug

conspiracy plus money laundering, you get the additional enhancement. Then the other kind of paradigm, though, you see is that there is some connection and usual interdependence between the group conducting the unlawful activity and the money laundering. And I think it's actually completely required by the text of the statute itself that you have that. And I will tell you why.

The Court asked about financial transactions, and the Court also read from the very beginning of (a)(1). Someone has to conduct the transaction knowing that it has the SUA in it. And when the government came back here and said, well, we don't need DPRK, because, of course, Mr. Storm had no contact with DPRK. That is not alleged. He didn't agree to conduct their transactions. Once you have severed that, you don't have a co-conspirator who is actually knowingly conducting transactions with the proceeds of a crime. You don't have it.

So, they attempted to broaden, and your Honor asked about the financial institution, they attempted to broaden what a financial transaction is here and said it's not just a financial institution, it also includes essentially a fire transfer, a transfer of funds by wire. Those transfers, of course, here are only happening -- that is what is happening with the protocol itself. And the only people who are knowingly conducting transactions, specific transactions, knowing that they contain the proceeds of SUA, are the illegal

bad actors, not Mr. Storm, not anybody with respect to Peppersec.

And that's true even if you span out and look at the UI as well. The UI itself also is agnostic to who is conducting the transactions. Mr. Storm does not know. And the UI itself is not conducting the transactions, only the protocol is conducting the transactions.

So I think you fail right at the beginning. I don't see any case, your Honor, where you have a third party conducting transactions, and then you have alleged co-conspirators over here who don't know exactly what is being transferred at any one time; they are not connected to those transactions. I see nothing.

There is a case the government cites *Gamez*. And in the *Gamez* case, there is a law review article there cited, and it says, "When money laundering statutes are used against third parties, who are not responsible for the underlying illegal activity, proving knowledge of the funds' illegal source becomes more difficult."

And I think that's exactly the tension here, your Honor. We have jumped completely away from what money laundering was intended to cover here. We actually don't have a co-conspirator who is doing a financial transaction, conducting a wire transfer in and out of that protocol, knowing that it contained SUA, the proceeds of SUA.

And I don't think the government can disagree that that's the standard. I look at paragraph 78 in the indictment and it says, "It was a part and object of the conspiracy that Defendant Roman Storm, the defendant, Semenov, the defendant, and others known and unknown"——and that's referring to co-conspirators——"knowing that the property involved in a financial transaction would and did conduct and attempt to conduct such a financial transaction."

Once you move past a co-conspirator doing that, I am not saying, your Honor, that you can't agree that as part of your conspiracy one of your co-conspirators does it. I am sure your Honor is familiar with sometimes the jury instruction language that says, a person did this, and then the defendant conspired with that person and joined the conspiracy knowing of its illegal object. We have that language in the 371 context. But here, your Honor, we don't have that. We have a third party. And once you get to that, then we are in an agnostic space. We refer to this as an agnostic protocol. The UI is agnostic as well. And in there, we are not even in the heartland of money laundering at all.

I took a turn last night on the FinCEN website, and if you look at the history of money laundering, and then the BSA rules that we know today on AML and KYC, you see that the money laundering laws didn't come into existence until 1986. And what we really know today is KYC and AML came because the

government felt, the governments of the world felt that they had not sufficiently constrained inputs into the money system from agnostic participants, people who were engaged in the financial services industry but didn't care whether they dealt with money launderers. The Western Unions of the world, your Honor, were not regulated until at least the 90s. The MSB requirement of a CTR doesn't come into place until 1994. And then the Patriot Act and its progeny after 9/11 started in 2001.

So what I would submit to the Court is money laundering is actually the highest standard here, the one that you really can't meet when you're actually talking about your standard Western Union, your standard MSB. And so the government has come up with laws to try to restrict ways into the financial system. And that's where you can get 1960 and the BSA and the specific money services businesses laws.

And it just so happens, your Honor, that now we are in a new space, with new technology, and Congress has not reached it, and the existing laws do not reach it. And I think this is a question of first impression for the Court, not just in 1960, but as to all of these. Because the government is trying to take conduct that it doesn't like, that it views as not compliant——and, your Honor, I heard a DOJ official speak about this, and they viewed it as a compliance case. But the problem is that the laws that they have on compliance and the BSA just

simply don't reach this, not yet. So as a policy they are asking the Court to use judicial authority to extend these statutes where they were not meant to go.

THE COURT: One moment.

Are you discussing in any way immutability or did you leave that with your colleague?

MS. AXEL: I think immutability also comes up in the conspiracy to commit money laundering in light of the dates charged. Again, the immutability for the Tornado Cash protocol, which is the pools, if you will, your Honor, in their vernacular themselves, that software is finalized in May of 2020, and the alleged conspiracy begins in September 2020. I do think, your Honor, that date shows that you can't have an agreement to commit the law when the protocol that is the thing that accomplishes the transactions was already done at that point in time.

So I do think the timing undermines the government's allegations of an agreement to an unlawful objective.

THE COURT: All right.

You speak about the IEEPA charge as well, and you are seeking to place Tornado Cash within the informational materials exception. The question I have sort of harkens back to what I was saying to Mr. Klein a little while ago. It's not clear to me the degree to which I can discredit or look away from the allegations in the indictment, including, in

particular, the charging language, which we all agree is correctly cited, and determine that something fits within the informational materials exception. Again, that to me seems to be the code, but I thought the government is telling me, or they will tell me, that this case is about more than code, it's about conduct using the code that's been developed.

So, I guess I don't know that I have seen courts finding that software applications, something different than just code, fits within the informational materials exception. But you believe otherwise?

MS. AXEL: I'm sorry. What was the end of the question?

THE COURT: The end of it is, I haven't seen apps referred to as informational materials. You say code, okay. But when I look at that list, which one of you will tell me should be close to exhaustive or one of you will tell me is not exhaustive, but I just don't see Tornado Cash fitting within it. And even if I did, the government is telling me this case is about more than the Tornado Cash protocols.

So let me understand better, or perhaps now that I have told you the concerns I have, tell me why I should not have those concerns and why Tornado Cash falls within the informational materials exception.

MS. AXEL: I think, your Honor, I would refer the Court back to the two *TikTok* cases because I think they are

very, very close to what we have here. And I think that the Court can look past the word "services," which is a conclusory word the government uses, I think, and look at actually what facts are alleged. And I think those facts, your Honor, make clear that this app and this protocol, we might call the UI more like an app, and the Tornado Cash protocol itself do clearly fall within the informational materials exemption.

The government wants to say and distinguish *TikTok* as being something very expressive, because our kids go on TikTok and they post videos and this is definitely a core element of speech. But, in fact, the TikTok regulations, your Honor, were much more restrictive. They were designed to get to the commercial aspects of TikTok. And so, when that case came in, the government said the same thing as the government is saying here. That this was not core speech that was being enjoined. That the core speech could continue, but it was commercial aspects. And that because it was commercial, it didn't necessarily fall within the informational materials exception. And whether you are talking about services or the word commercial here, either way, both courts said, we are going to look past those labels. What you actually are doing through here is you are indirectly restraining speech, and it falls within the informational materials exemption.

I think Congress was pretty clear in 1994. I am old enough, your Honor, to remember what a CD-ROM had on it, and it

either had software or it had things made with software. And you had your Word documents, your Honor, that you took home to work on your floppy disk. So that is what we are talking about. Those were informational materials on that type of software.

So we think this falls within the heartland of what the informational materials exemption was meant to cover.

The Court didn't ask here about immutability, but I do want to touch on that.

THE COURT: I asked earlier about immutability.

MR. AXEL: As to IEEPA.

THE COURT: I meant it as to all of those provisions which were in your portfolio. So fine, go ahead.

MS. AXEL: I think the immutability argument is even stronger here, your Honor, given the date that they allege that this conspiracy began, which is in April of 2022. The app and Tornado Cash had been going for nearly two years at this point. So I think when you claim that there is a conspiracy to violate IEEPA, and you measure willfulness as of that date, when the protocol is immutable years before that fact, I don't see how you can make out a willfulness claim on that.

And willfulness, your Honor, the Court I know expressed some reluctance about getting to intent standards, but again, this is out of the heartland of any IEEPA case. This is the government reaching to find a theory that has never

existed before.

I would refer the Court to DeFi Education Fund's lengthy summary of cases. The IEEPA professionals out there, the sanctions experts are baffled that anybody would think that this is willful conduct, when you had no contact with the DPRK at all and you designed something that was long in existence that later they chose to use. I don't think we are at all close to an intention to provide services to the DPRK. And you need for willfulness a bad purpose, knowledge that conduct was unlawful.

We cited the statutory history of the Trading with the Enemy Act, your Honor, and I realize that goes way back to World War I. But even in the heights of World War I, your Honor, Congress was concerned about prosecutorial overreach and chose a very high standard. In every one of those cases, including *Griffith*, you see actual conduct that connected the defendant to the DPRK. In *Amirnazmi* that the government cites, the defendant went and met with Mahmoud Ahmadinejad. We don't have any allegations here that would show any deliberate choice to violate the law, much less to assist the enemy.

THE COURT: One moment. Perhaps I will hear from Mr. Casey now. Thank you.

MR. AXEL: Thank you.

THE COURT: Since you prepared for oral argument, sir, I will find some question to ask you. I wasn't going to

otherwise, but I feel bad.

Sir, let's talk about overbreadth. I didn't find the facial overbreadth arguments to be as interesting as the as-applied, simply because I feel as though by now some court somewhere would have struck down these statutes, but you are persisting with facially overbroad challenges. Would you at least concede it is a less strong argument?

MR. CASEY: Well, your Honor, I would concede it's perhaps a little less stronger than the as-applied challenges here. But we do think that given the unprecedented nature of the government's theory here, that it calls into question the applicability of these statutes and the possibility of the scope and the overbreadth that's possible here.

THE COURT: Let me say this, sir, and I certainly don't mean to be talking past you. To me, the point of facial overbreadth is that you're not thinking about the situation in which it's being deployed. You're just looking at the statute and it just can't be that it recites criminal conduct.

So I have had money laundering cases. I have not struck down that statute as overbroad. I don't know that I have had an unlawful money transmitting case. And my IEEPA work was as a prosecutor so it's been a while. But I feel as though there are prosecutions that have been sustained in this district and in other courts which would suggest that a facial overbreadth challenge would not work. That's why I am

suggesting you focus your efforts on the as-applied.

In that regard, what you say to me is that these statutes are, in this case at least, content-based regulations of constitutionally protected speech.

Now, this is the issue that I was discussing with Mr. Klein a little while ago, which is you keep focusing on the idea, on the software, on the code, and the government keeps focusing on the conduct. So could you help me to understand why the government's functional capabilities argument does not save them in this case?

MR. CASEY: Sure, your Honor.

So, the Second Circuit in *Corley* recognized that computer code is a form of speech that's protected by the First Amendment, your Honor. And in *Corley*, the court recognized three ways that the code can have communicative content -- excuse me, the ways in which the computer program can communicate through the code. The first of those is to the user of the program; the second is to the computer; and the third is to another program. And to the extent the government is arguing that its indictment is aimed at the functional aspects of the code, that would go to the second form of communication, to the computer.

But in *Corley*, your Honor, the court held where the prohibition applied to computer codes solely because of its capacity to instruct a computer --

THE COURT: I will ask you to slow down.

MR. CASEY: In *Corley*, the court held that where the prohibition applied to a computer code solely because of its capacity to instruct a computer, the regulation is deemed content neutral.

And here, your Honor, it's worth noting that the government's own theory in its indictment is that Tornado Cash is considered a multi-part service that includes websites that provide information and access to the software code. So it's clear here, your Honor, the government isn't targeting just the functional aspects of Tornado Cash, but it's going to the heart of the message that the Tornado Cash project itself conveys.

THE COURT: Pause, please. I want to make sure I understand that. Not just functional aspects but the content. Let me understand that better. Just give me a little more detail.

MR. CASEY: Sure. It may help if I discuss what was decided in *Corley*. In *Corley*, the issue there was software that decrypted DVDs and allowed the user to essentially gain unauthorized access to the video content that resides on the DVDs. That, your Honor, is more akin to malware with no legitimate purpose. And while the court there still found that there was a speech component to that code, the prohibitions there were targeted against the software's nonspeech components.

In contrast, here, your Honor, the software does have a legitimate purpose, and it is designed to assist users in exercising their constitutionally protected right to maintain confidentiality over their private financial information, which is something the Second Circuit has also recognized. That in itself is a form of protected expression. As the Coin Center brief points out, the Tornado Cash suite of software itself carries a political message that people should be able to make private peer-to-peer transactions online without having to put their trust in traditional intermediaries.

THE COURT: I do want you to pause there, sir. That's where you started losing me. I appreciate that what you're suggesting is that Tornado Cash has a message about the importance of privacy and the promotion of privacy. But if it existed for the sole purpose of allowing bad actors to launder their funds through it, the promotion of privacy might give way to the fact that it's being used for criminal purposes. You could look at it and say, here is a very noble message that it's communicating. I might look at it and say, it is a haven for criminals. And we would both be right. So I am not sure how I get to look at this idea that I must accept its privacy vindication, or the idea that it vindicates privacy interests, above the bad things it's allowing people to do. Tell me why I can.

MR. CASEY: Your Honor, I believe that the cases cited

by the government to argue that the First Amendment is not implicated where software is used for criminal purposes, those cases all involve malware, and those have no legitimate purposes whatsoever.

THE COURT: This is what you said earlier.

MR. CASEY: Whereas the contrast here, there is a legitimate purpose and an expressive purpose in the code itself, as well as in the websites that talk about it, and provide access to information about the code, your Honor.

THE COURT: One moment, please, sir.

Those were the questions I had for you. Is there something else you need me to know?

MR. CASEY: No, your Honor. I would just emphasize again that there is in the Second Circuit a constitutionally recognized interest in maintaining confidentiality over one's financial transactions, and that also should affect, to your Honor's point earlier, why is this piece of software different.

THE COURT: Thank you, sir.

Mr. Rehn, thank you. Will you be going to the podium?

MR. REHN: I will go to the podium.

THE COURT: Okay.

Sir, you will let me know if I have been misstating your arguments to defense counsel this morning into afternoon. But as I understood it, the government's theory of culpability was not that Mr. Storm developed or participated in the

development of Tornado Cash, but that he and his colleagues developed and marketed and paid for and operated Tornado Cash, made lots of money in the process, knowing that Tornado Cash was being used to launder criminal proceeds, and, indeed, that Tornado Cash could be used to conceal the proceeds and to frustrate the efforts of law enforcement and of victims to uncover those proceeds.

Is that your argument?

MR. REHN: That's correct, your Honor.

THE COURT: Go ahead. I would like to unpack the argument, but if there is something you want to say in response, I will hear you now.

MR. REHN: I just want to make the point that the indictment clearly alleges that the Tornado Cash service was an integrated service that composed a number of features. And we openly acknowledge that one of those features——namely, the smart contracts in which the pools commingled customer deposits——became immutable as of May 2020. But there were a number of other features, including the website, the user interface, the relayer network, the TORN tokens that enabled them to make profits from the enterprise, and other features, all of which the defendant and his co-conspirators controlled during the relevant time period, and, in fact, made a number of changes to during the relevant time period in order to make Tornado Cash more popular and more profitable.

THE COURT: What you just said to me answers in part the next question that I have, but I want to make sure I understand this as well.

Looking at the indictment, I think the earliest charges begin in September of 2020, and that is the money laundering conspiracy. And given what I understand to be the sequence of events, it doesn't appear to me that the government is arguing or ascribing criminal culpability to the mere development or the initial development of Tornado Cash. And I guess I am understanding, instead, that you begin to find culpability when Mr. Storm and others operator Tornado Cash with knowledge that there were hacking episodes and being told by the victims that either -- I don't think they were occurring on Tornado Cash, but that the proceeds of them were being laundered through Tornado Cash.

Do I understand that?

MR. REHN: That's correct, your Honor. In order to sustain a money laundering conviction, we will have to prove that the defendant had knowledge that transactions involving criminal proceeds were occurring. So the timing in the indictment is timed to when it is very clear. There may well be evidence before that time, but certainly by no later than September 2020 the defendant was on explicit notice of large-scale criminal proceeds being laundered through the Tornado Cash service, and continued to operate and profit from

those transactions.

THE COURT: Now you're anticipating my next question, which is you're not suggesting that Tornado Cash was created in the first instance to facilitate money laundering. What you're saying, I think, is, if you have a service and you learn that that service is being used by bad actors to facilitate money laundering, that suddenly you become a participant in a money laundering conspiracy. Yes?

MR. REHN: That's correct, your Honor. And in that respect, the restaurant hypothetical that your Honor gave earlier is exactly on point. Any legitimate business that becomes aware that its financial transactions are being used to conceal the proceeds of unlawful activity, and continues to engage in those transactions knowing that they are commingling criminal proceeds with potentially legitimate proceeds, is participating in a money laundering conspiracy at that point.

THE COURT: That's a lot. And I want to make sure I understand that. Because I am not sure what you expected Mr. Storm and his colleagues to do. Should they have shut down Tornado Cash? I am not sure that they knew ex-ante that a particular transaction was money laundering or not. So how do you saddle him with criminal liability for not knowing in advance that this is what it would be used for?

That's the first of my concerns. So answer that, please.

MR. REHN: In respect to that concern, that's part of why the indictment time frame is what it is. I actually expect there is likely to be evidence at trial that the defendants did understand and anticipate that a large part of the market for the Tornado Cash service was likely to be criminal actors. But it's at the point of which you know that the transactions you are actually conducting through your business are, in fact, criminal proceeds is when we tie the money laundering conspiracy to begin.

THE COURT: All right. But is there some sort of tipping point? This is a service that I understand has more than one customer. It has hundreds, thousands of participants in the Tornado Cash service? I don't know. Do you?

MR. REHN: We have some evidence as to the number of transactions, the number of wallets that transacted with it, but that doesn't necessarily tell us how many individual actors or entities.

THE COURT: Fair enough. Let's try it this way.

If Tornado Cash had one customer, one and only one, and that customer was a foreign government subject to sanctions, or a noted drug dealer, or an obvious fraudster, I can understand you saying, at the point that Mr. Storm and his colleagues allowed this bad actor to continue to deposit or to process or mix funds through Tornado Cash, that he was at that moment participating in money laundering. I understand the

argument.

My concern is, if Tornado Cash has a thousand customers and one of them is a bad actor, and those transactions get processed through Tornado Cash, are they criminally liable? What if it's half of the customers? What if it is two-thirds of the customers? I can give you whatever fraction you want. What I am asking is whether there is some tipping point at which, in a situation where you have multiple customers, your knowledge that one of them is depositing the proceeds of criminal activity makes you liable for money laundering? This is the concern I have.

So, here, is one customer enough?

MR. REHN: Well, it depends on the facts and circumstances of each individual case. But certainly a single transaction as to which a defendant has knowledge is designed to conceal proceeds and the defendant knowingly participates in that transaction has been held to be sufficient evidence.

When you're talking about a business like this, though, and especially a business that is a financial institution, the law and a number of prosecutions require that there be protocols and procedures put in place to address that risk and to attempt to prevent those transactions from going on on an ongoing basis.

THE COURT: That's a question I am going to ask you later. Well, I will do it now.

Is Mr. Storm being prosecuted because he didn't have anti-money laundering or know-your-customer protocols?

MR. REHN: That was one of the requirements of the business that he would have had to implement under the money transmitting laws.

THE COURT: Yes, of course. But that doesn't make him a money launderer, does it?

MR. REHN: That's correct. With respect to the money laundering, however, it is relevant that he did not take any steps to attempt to prevent himself from continuing to conduct transactions in criminal proceeds. And as to that, it isn't really different from a non-financial institution. So the restaurant example again. If the restaurant knows that one particular waiter is depositing criminal proceeds along with their tips at the end of the day, they have an obligation to stop that particular thing from happening, regardless of the percentage of their revenue that the business constitutes. If they are aware that there is a particular actor that is committing money laundering, they are by then conducting transactions that commingle those criminal proceeds helping to conceal them.

And that's exactly what is alleged here. There is a number of specific hacks the defendant is on notice of and getting complaints from victims. There will be evidence they got inquiries from law enforcement --

THE COURT: Slow down, please, sir.

MR. REHN: There are many ways in which the defendant and his co-conspirators are aware a large number of transactions, well over a billion dollars, as alleged in the indictment, are being laundered through the Tornado Cash service. And they do nothing to screen potentially legitimate transactions from the ones that involve the proceeds of these crimes. And there is a number of steps they could have and we argue legally required to take to address that risk. Those don't necessarily have to be perfect. Every financial institution doesn't necessarily have perfect measures. But the fact that they engaged in this conduct and profited from it at this level, and continued to do so in full knowledge that that was what was going on, does give rise to criminal liability under the money laundering statute.

THE COURT: You spoke again about how they profited, and I know there is a dispute between the parties as to the degree of profits. But are you suggesting that if Mr. Storm forwent any profits from these deposits into Tornado Cash, he had pride in what he had created and didn't see a need for further financial remuneration from it, do we not have this case? If he didn't realize any funds from it, do we not have this case?

MR. REHN: We may have an issue with the 1960 charge in that instance. But we wouldn't have a problem with the

money laundering count, because it's not an element of the offense that you profit from it.

I think the reason I am coming back to that is, it is evidence of his bad intent and his willingness to continue to engage in it. And there will be evidence that a very high percentage of the Tornado Cash transactions were, in fact, criminal and that the defendant understood that and, in fact, he and his co-conspirators understood specifically that taking steps to address that would hurt their profitability. So that will go to the degree to which this was a knowing violation of the law and the nature of the conspiracy that will be proven at trial. But I agree with your Honor that profitability itself is not necessarily an element of the offense. And you could imagine a philanthropic money launderer.

THE COURT: I will try to. Yes.

Let's talk about smart contracts. A focus of the defense motion to dismiss in this regard is that, because of the immutability of the contracts, there really wasn't anything that Mr. Storm was doing or could do as of late 2020 or April 2022. Do you agree with that? Because perhaps what you're saying is, agreeing with the idea that the pools were immutable, there were enough other moving parts that weren't, that that's what you're predicating liability on. Is that what the argument is?

MR. REHN: Your Honor, in this case, the liability is

predicated on a number of additional affirmative acts that the defendant was taking with respect to the Tornado Cash business throughout the charged time period. In fact, the business was not immutable. In fact, the indictment alleges multiple instances in which the defendant made changes to the Tornado Cash service. One important illustration of that is the pools were made immutable in May of 2020.

THE COURT: And eventually they went to open source.

MR. REHN: They are claiming that their user interface eventually went to open source. As to the pools, I think the code is sort of built into them on the blockchain so people can see the code earlier than that.

But as to the business, the defendant was raising funds from investors months after May of 2020, in August of 2020. And in his pitch to investors, he is describing his business and saying, we anticipate we are going to be able to monetize this and here's a few examples of how we are going to do that. Then, in December 2020, they start implementing those ways of monetizing the service. By releasing the TORN tokens, by beginning to develop the relayer network, ultimately deploying what is called a relayer algorithm. All of these are things designed to increase the profitability of the business, while also making it more popular because they enhance the anonymity that they are offering to their customers. And they are doing this in a context in which they are aware that in

doing so, they are only increasing the degree to which the Tornado Cash service effectively conceals the proceeds of what they now know is large-scale criminal conduct flowing through their business.

THE COURT: There is a degree to which I feel you're imposing criminal liability because of the failure to make changes. We talked earlier about the failure to implement or to have anything resembling know-your-customer rules or anti-money laundering rules. Are you arguing criminal liability from the failure to make changes to the UI?

MR. REHN: We are arguing criminal liability from the participation and continued transactions knowing that they involved the proceeds of criminal activity, through, among other things, the user interface as well as the relayer network. And there will be both a general argument to the jury that the jury can come to the conclusion that the defendants had that intent from the fact that they failed to take any steps to prevent it. But, in addition, there will be a number of particular moments in time where the defendants are particularly aware of transactions involving the proceeds of criminal activity, and are processing those transactions through the user interface in full knowledge of that fact.

So a very prominent example alleged in the indictment takes place in December of 2021. There was hack of a cryptocurrency exchange. It's the single biggest deposit day

in the history of the service. And when that happens, all of those criminal proceeds flow into the service, a very strong majority of all the funds in the Tornado Cash service are, in fact, those criminal proceeds. So the subsequent withdrawals --

THE COURT: Stop. What should they have done?

MR. REHN: At that point in time, they are operating a means by which the criminals can withdraw the funds to clean cryptocurrency addresses. They can prevent that. They can easily say, we are going to stop those withdrawals because we know they involve these criminal proceeds.

THE COURT: But isn't there a degree of retrospectiveness to that issue? I don't know that they knew, on the day that it was their biggest deposit day, that it was going to be their biggest deposit day. So I am concerned about faulting them, and indeed imposing criminal liability on them, for a happenstance that a bad thing happened and that folks decided to launder the proceeds of the bad thing through Tornado Cash. Perhaps you are going to tell me that they not only knew that this could happen, it was a feature of Tornado Cash. But to say that I know at the end of the day this was their biggest deposit day doesn't give me insight into the fact they knew it was going to be or that they knew that this awful hacking incident would have its proceeds laundered through Tornado Cash.

MR. REHN: So I think I have three responses to that, your Honor.

THE COURT: Okay.

MR. REHN: The first is, they did in fact market the service specifically to money launderers. And there will be evidence of that at trial, and we think that will be one of the bases on which the jury can find the requisite intent to be a conspiracy to commit money laundering.

Just to take an example of that, the defendant created marketing materials that showed dirty ETH, and then it showed a washing machine, and the washing machine had the Tornado Cash logo on it. So it was very explicit what they contemplated their customer base wanted.

THE COURT: I will look forward to the demonstrative exhibits if this goes forward.

MR. REHN: Secondly, there will be evidence that the Tornado Cash service sort of exploded in popularity and there was huge discussion, both publicly and among the defendant and his co-conspirators, that the source of that explosion and popularity was the fact that it was such a useful tool for hackers and money launderers. They saw it over and over again, everybody sees our service as a tool for hackers and money launderers.

In fact, they are sending each other examples of people who have been prosecuted for similar conduct. So in the

fall of 2021, Storm actually sent a news story about the Silk Road case to his co-conspirators and said, I understand one of our developers just quit because this is all about hackers and money launderers. So they have this knowledge that the business as an ongoing enterprise is a money laundering enterprise. So I think that could also be the basis for finding a money laundering conspiracy.

Then, third, even if that wasn't enough, which I think it clearly is, it's not just the deposits. So, yes, it's not necessarily the case that the defendants knew that this cryptocurrency hack would happen in December of 2021, and then the hacker would deposit those specific proceeds on that date. But it's the subsequent withdrawals as to which they are on notice, before those withdrawals happen, that people are going to be withdrawing criminal proceeds, and they are in a position where they have every opportunity to not process those withdrawals, because they control the user interface and they can implement measures to prevent those withdrawals from happening. Every withdrawal in the subsequent days and weeks until those criminal proceeds were out of the service involved criminal proceeds. Maybe commingled with a lesser percentage of some legitimate proceeds, but those withdrawals themselves certainly involved criminal proceeds, and they were fully on notice of those specific ones during that incident.

THE COURT: You mentioned Silk Road a moment ago, the

Ulbricht case. You suggest to me that that is a useful comparator in this case, but I thought I understood that Silk Road was developed from the start as a place for criminals to facilitate their transactions. Once again, this case differs because Tornado Cash, at least you're not yet alleging that its genesis was the desire to facilitate criminal conduct. So perhaps you're saying that Silk Road is useful insofar as contemporaneous references to it by Mr. Storm and his colleagues show knowledge, intent, absence of mistake. But I didn't see that Silk Road was on all fours with this case. Are you suggesting that it is?

MR. REHN: I think that's a fair point, your Honor. I don't think we will necessarily attempt to prove that the defendants from the very outset, when they first came up with the Tornado Cash service, were specifically viewing it as a criminal enterprise from the outset, necessarily. The evidence may support that finding. But even without that, I don't think *Ulbricht* turns out differently if Ulbricht comes up with the Silk Road concept, and after operating it for a few months realizes that his customer base is all criminals, and then starts marketing to them and is specifically profiting from those transactions in full knowledge that they are taking place. And the language in the *Ulbricht* case about, it is as if the defendant put out a notice to the whole world, you're welcome to come and launder your criminal proceeds on my

website, is exactly the case here. The defendants, both explicitly and implicitly, were sending that message to the criminals of the world. This is a great opportunity to conceal your criminal proceeds. All you have to do is pay us a little fee when you withdraw them.

THE COURT: The washing machine seems like an interesting metaphor.

Let me ask a question that goes back to sort of my initial questions to you.

So let me ask you to think about something like WhatsApp. As I understand it, one of the great benefits of WhatsApp to those who use it is that the communications are encrypted. They are harder to intercept. They are harder for law enforcement to monitor or intercept. So I have had cases where participants in the criminal conduct specifically used WhatsApp in order to avoid law enforcement detection. WhatsApp must know that one of its great selling points, the encryption component, allows it to be used by folks engaged in criminal conduct. But I don't see you charging WhatsApp with criminal offenses. So what is the difference between the folks who operate WhatsApp and the folks who operator Tornado Cash that makes you believe the latter are subject to criminal liability?

MR. REHN: Well, I think there are a few reasons for that, your Honor. One important distinction is that on WhatsApp all the communications are, as I understand it at

least, encrypted and not visible to the operators of WhatsApp. And so, while WhatsApp may have some statistical inference that some percentage may be criminal communications, it doesn't have any specific knowledge of any particular criminal communications.

THE COURT: Sure. But if the AG wrote to WhatsApp and said, by the way, we have had X thousand prosecutions this year, and fully 50 percent of them involved the use of WhatsApp in order to encrypt communications and thereby make it more difficult for law enforcement to find or uncover criminal activity, please stop this, and they said no, they are on notice. This point you're giving to me is, by not having them visible, perhaps the WhatsApp folks might not know. But if you told them, then they have to know. Does that change your belief that that does not result in criminal liability?

MR. REHN: It doesn't because of the encrypted nature of it. Even if they knew that a very large percentage were criminal, they wouldn't necessarily be able to sort out the wheat from the chaff; they wouldn't have a way of doing that.

THE COURT: And you believe Mr. Storm could do that?

MR. REHN: Absolutely. In fact, the indictment alleges an instance in which they attempted to do so involving the Roman network hacks, where they did in fact implement a change to the user interface to screen out deposits directly from sanctioned wallets.

Now, there will be evidence that that was a pretextual PR move, and they understood that that would be ineffective. But they could have also implemented a number of other measures to be more effective, including requiring every depositor to identify themselves, as well as doing screening going back further than the first transaction deposit. So there are a number of things they absolutely had the ability to do.

THE COURT: If you have other reasons why WhatsApp was different, may I hear them?

MR. REHN: Well, I do think that the regulated context in which this case occurs is relevant not just to the 1960, but to the 1956 charge as well. Because one reason the government cannot require WhatsApp to maintain records of its users has to do with the fact that WhatsApp provides expressive activity and there are First Amendment reasons.

THE COURT: Eventually you are going to tell me why this isn't an expressive activity.

MR. REHN: Courts have upheld for many decades the government's ability to require financial institutions that process financial transactions to maintain data. Yes, there is a lesser constitutional interest in financial privacy, but it's certainly constitutional for the government to require institutions that are processing financial transactions as a business to maintain customer information and anti-money laundering measures and the like.

THE COURT: Turning now to the money laundering charge. I understood, and still understand, that the defendant doesn't have to actually be involved in the actual conduct of the underlying unlawful activity, but just has to be aware of the funds and proceeds of a specified or unlawful activity.

The concern I have again, though, is the idea of the scale of the Tornado Cash enterprise and how you evince agreement with a particular bad actor when you have so many actors on the platform. So I would like you to help me with that, and then I will probably ask follow-ups as need be.

MR. REHN: Certainly, your Honor.

The government is not required to prove an agreement with the people committing the specified unlawful activity. As far as the government is aware, there is no case that has ever held that that's a requirement of the statute. When the jury will be instructed on the elements of money laundering, there will not be an instruction that the defendant must have conspired with somebody who committed the specified unlawful activity.

THE COURT: Did I understand correctly from Ms. Axel that the results of her search were that --

Ms. Axel, this was regarding money laundering, correct?

MS. AXEL: Yes, your Honor.

THE COURT: Her search suggests that the defendant in

question either was also a participant in the underlying activity or that there was some mutual interdependence. Are you suggesting that neither of those is required?

MR. REHN: That's correct, your Honor. And there is no case that has ever held as such. In fact, just to take sort of an obvious example, the *Stavroulakis* case, the defendants conspired with each other to launder proceeds, which they understood to be the proceeds of the specified unlawful activity, but the person providing them with the proceeds was a government agent acting undercover. So they couldn't possibly have had a conspiracy with anybody committing the specified unlawful activity, because you can't conspire with an agent of the government to break the law. So that's sort of an obvious case where there was no such requirement.

But there are a number of prosecutions, both in this district and throughout the country, involving third-party money launderers who understand that their businesses are receiving and concealing criminal proceeds, but don't necessarily form a specific agreement with any one of those criminal actors. These are very common cases where there are whole networks of people moving money around on different shell entities and things like that in order to conceal what they understand are criminal proceeds, and not all of those people, or maybe even not any of the people in the networks, have formed an agreement with the actual criminals.

THE COURT: The concern that remains for me, and maybe you will be able to dispel it, is that, again, perhaps I am misperceiving the size or the complexity of Tornado Cash, but I am worried about imposing criminal liability for money laundering based on negligence, not conscious avoidance but actual negligence. Perhaps you will say to me, fear not, Failla, because the evidence at trial will show that this isn't negligence and they absolutely knew what they were doing. But please understand the concern I have. Mr. Klein, and perhaps Ms. Axel, spoke about liability predicated on negligence. I wish not to have people convicted of federal criminal offenses based on negligence. So give me some comfort that that is not what is going to happen here, and not merely based on the evidence in your case, but based on the construct of bringing cases of this type in this setting.

MR. REHN: Yes, your Honor.

We would first say that it really isn't this case. Second, I would just say that that is an issue to be resolved based on the proof at trial, and certainly not a basis on which to dismiss the indictment. It would be, I think, unprecedented for a court to say, I don't think you will be able to clear the negligence versus criminal conduct bar at trial so I am going to dismiss this count.

THE COURT: By the way, if I had a nickel for every time somebody tells me that this is unprecedented, I could

retire. It would certainly exceed my government salary. They think your prosecution is unprecedented and you think dismissal of the prosecution would be unprecedented. I accept that you all feel this way.

Go ahead.

MR. REHN: But this case is precedented. There is the *Ulbricht* case we have talked about. There is the *Sterlingov* case in the District of Columbia. There are number of cases in which defendants who operated services like these, that were primarily of use to criminals seeking to conceal their criminal proceeds, were found to be criminally liable. And there is no wave of cases in which the government is going after sort of innocent actors because one criminal managed to slip a little money through their program. There are not examples of that. And the reason is because we understand we will have to prove beyond a reasonable doubt that the defendants formed the intent to join a conspiracy to launder the funds of unlawful activity. And in proving that, we will present direct evidence that these defendants were specifically aware of both the general use of their service and a number of large-scale specific instances in which they were, in fact, laundering those funds.

So I don't think that there is some sort of concern about a hypothetical prosecution that is raised in this particular case.

THE COURT: I might still have those concerns, but I

appreciate your belief that this is not the case where those concerns should be manifest.

Mr. Klein and I had thoughtful discussions about the 1960 count, and he is quite convinced that control has to be shown, and that it can't be shown here because of the immutability issues we have been discussing earlier. You have said to me in response that control is not necessary and that there are other factors that may be considered.

Tell me, please, what I can look at to give me the same comfort that I would have if there were evidence of control. Perhaps I should ask the antecedent question which is, you're not claiming control of the funds here, correct?

MR. REHN: Your Honor, that's the one issue as to which we think there is sort of a legal question presented by these motions to dismiss. If the Court were to find that control of the funds was absolutely required, we would not be able to prove control of the funds at trial.

And there's a number of reasons why that proof is not required under the statute. As a matter of sort of first principles, it's the language of the statute. There is no language that suggests that control is required in the statute. In fact, section 1960 uses the word control, but in reference to control all or part of the business, and it doesn't say anything about control when it's talking about transferring funds on behalf of the public. No case has ever suggested that

control is an element of the offense -- control of the funds being transferred is an element of the offense. And it's contrary both to the text of the statute and the intent of Congress to pass a statute that applied to this sort of marketplace activity not any particular technological means of accomplishing it. And it would really defeat the intent of Congress if we were to import that sort of an attextual limitation and prevent the statute from being applicable in this context.

THE COURT: What am I going to see instead? What is the proof going to be instead?

MR. REHN: The proof will be that the defendant's business transmitted funds from one cryptocurrency address to another by conveying instructions to the blockchain to accomplish those transfers. And that is very similar to a number of other 1960 prosecutions that have taken place. There is the *Murgio* case from 2016, the *Harmon* case from 2020, the *Sterlingov* -- those latter two are District of Columbia cases. But in all of those cases, the courts held that if the government is able to prove that the business at issue enabled its customers to transfer funds from one cryptocurrency address to another, that is money transmitting. I think in the *Harmon* case there is a reference to the fact that Harmon controlled the intermediate wallet. The court doesn't suggest that that is a requirement of what the government would have to prove at

trial. And, in fact, in *Murgio* and *Sterlingov*, there is not even a reference to that as being one of the facts in the case.

So, it is not something that courts have held is something that the jury has to find. What we will have to prove is that the business was involved in transferring funds on behalf of the public, and it's clearly the case here. As we have discussed, the way that a transfer of funds happens on the blockchain is that instructions are communicated to the network of computers that make up the blockchain. So prior to those instructions being communicated, the wallets on the blockchain have one balance of funds. After the instructions are communicated, there is a different balance of funds in accordance with the instructions. The instructions that conveyed that transaction, that conveyed that transfer of funds in this case, are accomplished by the defendant's user interface and other contracts the defendant created and controlled, as well as the relayer network, which the defendant created, exercised a degree of control over, and conspired with the other people who were involved in that network.

THE COURT: I suspect I shouldn't be asking this, but it's not stopping me from asking this. Would you agree that the most aggressive or the least traditional of your charges is the 1960 charge?

MR. REHN: I think that with respect to this control question, the defendant's argument is novel in that no court

has really addressed this argument before. I am not aware of a defendant making this argument before. There are no cases they have cited where a court has held that control is required. So in that sense, it's sort of new in the sense that no court has addressed it. We don't think it's novel in the sense of this is a novel application of the statute. The intent of Congress is manifest. It didn't care about the technological means by which the funds are being transferred. That wasn't what Congress was concerned about. That's why the statute was passed decades ago and has been applied repeatedly to cryptocurrency businesses.

What Congress cares about is the economic function that these type of businesses serve. What that economic function is is they allow customers to move money around. And the concern is that if you don't have certain anti-money laundering and know-your-customer protections in place for those type of businesses, it allows criminals to exploit those businesses to conceal the crimes. So congress put in place a regulatory regime to address that, and that regulatory regime was meant to be generally applicable to businesses of this type.

And the defendant doesn't dispute that his business is functionally identical to the businesses at issue in *Faiella*, in *Harmon*, and *Sterlingov*. What he says is, because we designed our system so that we don't see the note during the

transfer, that means we technically didn't have control of the funds, and so you can't prosecute us. But there is no reason on offer why Congress would have wanted statutory liability to turn on such an arbitrary distinction when the economic function of the business is exactly the same.

THE COURT: Let's turn perhaps finally to the issue of due process arguments. You heard me speak with Mr. Klein about the difference between Rule 7 and Rule 12. They are not arguing that you haven't tracked the language of the statute. I didn't see a request for a bill of particulars. I think they understand what the issues are. But I think their concern is this broader one, and that is that it's not necessarily clear to folks operating in the cyber or crypto spaces that conduct of the type alleged here can subject them to criminal liability.

So, on an issue of fair notice, how is it that Mr. Storm or someone in his position should have known, for example, that he should have stopped these transactions, or that he should have employed know-your-customer, anti-laundering protocols, or something like that. Or, if you would like, let me say this a little bit differently. Even if I find that the statutes are not facially ambiguous or facially overbroad, can't I have the concern that in this setting they are being applied in a way that people did not expect and could not have expected?

MR. REHN: Your Honor, I don't think that's true. I think there's different aspects of that with respect to each count.

THE COURT: Please.

MR. REHN: So, first with respect to the 1960 charge, as I have now said several times, there are multiple prior, very similar prosecutions, and defendants were on notice of them. And there will be evidence that this defendant in particular knew about those cases and, in fact, discussed, oh, do we need to start complying? And the answer was, no, there is no obligation, that would hurt our market share. So there is going to be evidence of that at the trial.

But, more generally, this is actually -- we have seen this repeatedly in these cases where cryptocurrency businesses in particular have come in and said, oh, the statute shouldn't apply to my conduct because I didn't know that it would apply to my conduct. The first case I think was the *Faiella* case where the argument was, well, cryptocurrencies aren't funds. And that was a loser because under the plain language of the statute they are.

And there have been similar attempts to try to prevent what appears to be a plain application of the statute from applying to a new type of business. And that's simply not what due process requires. Due process requires that the statute's application to the conduct be clear from the language of the

statute. But it doesn't require that the government never bring a case in a new technological context. The wire fraud statute was passed decades before the dawn of the internet. It certainly couldn't be the case that that is what due process means. And there will be ample evidence that the defendants engaged in conduct that is a clear violation of the statutory language, which is really what is required.

Briefly, I think a similar analysis applies to the money laundering. I did want to mention on the IEEPA theory, the defendant himself, when he was on notice that the Lazarus Group's sanctioned wallet was using the Tornado Cash service to launder its funds, told his co-conspirators that they face criminal liability for this. So he was certainly on notice that engaging in these transactions involved criminal liability.

Now, what they chose to do was put a Band-Aid on it and make a public statement that they had addressed the issue, while then profiting to the tune of millions of dollars from those transactions over the subsequent weeks. But they certainly were fully aware that they faced potential criminal liability, and that's why they did what they did, and the evidence is going to show that at trial.

THE COURT: Anything else, sir? Anything that I asked your adversaries that you wish to speak to? And then I will have the briefest of reply from my friends at the back table.

MR. REHN: Let me just check my notes briefly.

I will just make one point. It doesn't sound like the Court will reach this issue. But on the money laundering charge, as we have explained, the transactions were conducted through the user interface, which participated in conducting those transactions by conveying those messages to the blockchain. Even if the Court accepted everything that Ms. Axel said about that issue, there still are transactions involving criminal proceeds in this case, and those are the relayer fees. Because when those transactions occur, the relayers take fees out of the funds being withdrawn. So the funds being withdrawn involve criminal proceeds, and then the relayers take a portion of those funds involving criminal proceeds. The relayers keep a portion for themselves and then they kick back some of the proceeds into the TORN token holders.

So those transactions, which are unambiguously involving participants in the conspiracy, at a minimum, are transactions involving criminal proceeds. We think the whole thing are transactions that the conspirators are participating in involving criminal proceeds, but even if you looked at just those transactions, there is no question there.

THE COURT: Thank you.

MR. KLEIN: I will stay here to speed it up.

THE COURT: We run as long as we need to run. I have

a sense of your arguments. They have been exceptionally well presented. But I will hear from you.

Go ahead, sir.

MR. KLEIN: 30 seconds on the 1960.

There are no cases, of the ones the prosecutor cited, *Murgio*, which I was involved in representing Anthony Murgio, and the others, they all involved --

THE COURT: Microphone closer to you, please, sir.

MR. KLEIN: They all involved control. Every single case. The reason why this is raised for the first time here is because this is the only case ever with a 1960 prosecution where the defendants didn't have control of the funds, period. There is no case where that is not the case. The *Sterlingov* case, the *Murgio* case, every case they cited to you, the person had control. They were a centralized intermediary. So they are radically different. And that is exactly why FinCEN has the software provider exemption, for this exact kind of case. That is what that exemption speaks to. When you are just providing the tool, which it was, to do something, you shouldn't be prosecuted, you shouldn't be held accountable. And that's where we are with 1960.

THE COURT: Thank you.

Ms. Axel.

MS. AXEL: Yes, your Honor.

First, with respect to the conspiracy to money

launder, a couple of quick responses. One is, again, your Honor, there is no case that we find that there is no link in the chain between whoever committed the substantive offense and the money launderers. The government comes in and cites -- it was the government informant case. And in that particular case, your Honor, still, that government agent provided that knowledge that the proceeds had come from a specified unlawful activity. It's a legal impossibility to conspire with a government agent so we have a legal impossibility problem. But, nevertheless, in terms of the link in the chain --

THE COURT: *Stavroulakis*.

MS. AXEL: -- that person provided that link so that you had, when the transaction was conducted by the money launderers, you had clear knowledge that they had involved SUA and an intent to join that agreement. And here, by severing the chain between the people conducting the transactions, knowing that they contained the proceeds of SUA, and the alleged conspirators, meaning Peppersec, we don't have that connection, and there is no case in the world like that.

I also turn the Court back to 1968(a)(1) and respond to the relayer point there as well. There, still, the relayers do not engage in financial transactions knowing that the proceeds involved are from unlawful activity. They also are agnostic. They are on the back end of the pool. They don't know who is the person that initiated the transaction. And the

nature of the pool itself of course breaks the chain, and we don't know what went into it. So you do not have an alleged member of the conspiracy who knowingly, knowing that the property involved in the financial transaction represented SUA, conducted that transaction. So it just fails money laundering out of the get-go.

Again, there were allegations about what could have been done. None of that shows knowledge that actually SUA was involved in particular transactions and the defendant conducted, caused, or conspired to conduct those particular transactions.

I don't know if I need to respond to the WhatsApp point.

THE COURT: No. Thank you.

MS. AXEL: Obviously, the Court is familiar with agnostic tools that criminals can use for ill purposes, and this is like those cases. *Ulbricht*, *Sterlingov*, and the *Helix* cases, all of those actually were centralized processes where you actually had the defendant in those cases touching transactions, receiving money from transactions. So you didn't have this problem that the person didn't conduct a transaction knowing that it involved unlawful proceeds. Those were all factually different.

Your Honor, in summation, we would submit that either this is a 1960 case or it's not. And what the government has

tried to do here is that they have stepped in to what is really a regulatory landscape, and they have acknowledged there is a legal issue as to whether Congress reached this conduct because the defendant did not control actually the proceeds that went through Tornado Cash. That's a legal issue. But that regulatory landscape is really what Congress intended to address this type of conduct. You can't skip past that strict liability regulation and then say instead, because we as the prosecutorial want to reach conduct we don't like, we are going to try to reach this much higher standard of intent and twist and violate the words of the statute. That is an unfair expansion and that, your Honor, also would violate fair notice provisions.

Finally, with respect to your Honor's standard, I would remind the Court of the *Aleynikov* case. You referenced Rule 12. In that case, it's a perfect -- well, nothing is perfect. It is an example that the Court can look to. In that case, Judge Cote dismissed one of three counts, the other two went to trial. And when it got to the Second Circuit, the court found the indictment was insufficient as to all three. Because in that case, as here, the government was trying to push sort of novel theories where the facts did not make out a sufficient indictment. And I think that's a good analogy for what we have here. Our counsel at the table here said, courts have allowed, of course, certain cases to be brought expanding

to new technology, but they have now pushed beyond the bounds of where the law allows them to go.

So, here, your Honor, this is not a case where the laws that we have reached this particular conduct. Other ones, they may have. But we also have seen courts in this district and elsewhere beginning to stand up to sort of new regulation by enforcement, and we would submit that that's what is happening here and that the Court should find that this particular prosecution goes beyond the bounds of the statutes.

THE COURT: Thank you.

Mr. Casey, last words?

MR. CASEY: Nothing to add.

THE COURT: This has been really interesting, and I know that's not what either one of you wanted to hear, but it is, it's interesting. These are very interesting concepts, and I want to take the time to think about them. I am sure someone will get a copy of this transcript, and I would welcome it immediately upon your receipt of it. I will try and get back to you as soon as I can, but I don't know when that will be.

That leads to the issue of a request for an adjournment of the trial. I am sure you're both right. The defense needs more time. The government thinks they have had enough time. I am thinking of this a little bit differently because I would like the time that I need to actually decide these very important issues correctly. So recognizing that

this is over the government's objection, it looks like I may have some time opening up in December.

Now, I have a trial Monday so that won't help you. I have a trial that was in October but it now looks like it's moving, and I don't think I have enough time to deal with this. So what I am looking at is, I think, beginning either of the first two weeks of December. What I don't know speaking with you is whether you think this is a two-week trial, a three-week trial, a two-month trial. None of us——really, I mean me——wants to have a jury concerned about holiday issues, but I have a trial that begins the first week of January, and that's a six-week trial, criminal, classified, lots of fun. I am not moving that. So if you said to me, this is a three-week trial -- also, let's be clear, I don't want to make this a February or March trial because this other trial, the January 1, who knows when it will end. I thought this was a two-week case, but I could be wrong.

MR. REHN: I think it's a two-week case.

THE COURT: I was looking at, I think the 2nd of December. Is there a problem with that, other than we will all have less pleasant Thanksgivings than we might otherwise? Does someone else have a scheduling conflict for the 2nd of December?

Mr. Rehn, if you want to jump up and scream about moving the trial, I get that you don't want me to do it. I am

taking the heat for this. It's not for them, it's for me.

MR. REHN: We understand, and the government is prepared to go to trial at our earliest convenience. We would prefer the date that the Court has scheduled. I think we are available if the trial were to start on December 2nd.

THE COURT: Mr. Klein.

MR. KLEIN: Your Honor, the defense is also available on December 2nd.

THE COURT: So, this is your motion to adjourn. I am granting your motion through the 2nd of December. We will issue a new trial scheduling order to count back as to *voir dire*, things of that nature.

Mr. Klein, something else, sir?

MR. KLEIN: Just because the Thanksgiving holiday is right before, and we all have families, I know how your schedule works, but I would prefer not to have to be in New York on the Monday, but I guess we will see what your schedule is.

THE COURT: Do you want to begin on Tuesday the 3rd?

MR. KLEIN: Yes, your Honor.

THE COURT: Can I still be done by the 13th, sir? I don't know what your case is. You may not know what your case is.

The answer is, I could do that, but I don't know how pleased the jury would be to go into a third week.

MR. KLEIN: You mean into the week of the 16th?

THE COURT: That is what I am saying.

MR. KLEIN: I wouldn't be pleased to go into that week either.

THE COURT: I like families too.

You can talk with the government. I will set it for the 2nd. As we get closer to, we will see where we are because we won't have done the summons yet for the jury. We will do a new trial order.

May I understand, is there an application from the government under the Speedy Trial Act? Did we not have time set through the trial date? It may have been that I excluded only through the date of today's proceeding. I am not remembering.

MR. REHN: I believe it was excluded through the trial date, although I don't have the order in front of me.

THE COURT: I can look.

MR. KLEIN: That's our memory too, your Honor.

THE COURT: Is there an application now to extend that?

MR. REHN: Yes, your Honor. In light of the Court's considerations of the issues raised by the defendant's motions, which actually I think the pendency of those motions may, in fact, toll the Speedy Trial Act.

THE COURT: It does. I am in the reasonable period of

time to resolve from the hearing, which would be about 30 days.

MR. REHN: In an abundance of caution, we would ask that the Court exclude time from September 23rd to December 2nd, to allow the Court to consider the issues, the parties to consider the Court's rulings on those issues, and to prepare for trial.

MR. KLEIN: No objection.

THE COURT: May I address Mr. Storm directly, sir?

MR. KLEIN: Yes, you may.

THE COURT: Mr. Storm, you have heard in prior conversations about the Speedy Trial Act, and I have excluded time in the past through the trial date based on the importance of everyone having the time that they need to prepare for trial. Here, there are certain periods of time that are excluded automatically, and that would be for the filing of motions, the hearing on the motions, and a certain period of time for me to decide them. I will be as prompt as I can in resolving these motions, but I also want to have the time that I need. I also would like to be sure that everybody has what time they need to prepare for this trial. And given that there is a request from your side to have it moved, I think it's only fair that time be excluded because one of the reasons given was that your counsel wanted time to review everything and prepare. So I am making a finding that the ends of justice served by excluding the period of time between that last date in

September and the 2nd of December outweigh the interests that you have and the public have in you getting to trial more quickly.

Do you understand, sir?

THE DEFENDANT: Yes, I do, your Honor.

THE COURT: I thank you.

Mr. Rehn, checking with your team, anything else we should be doing today?

MR. REHN: Nothing from the government, your Honor.

THE COURT: Mr. Klein, something else, sir?

MR. KLEIN: Yes, two things. One, we don't want to presume that we will be in trial. We are standing on our motions.

THE COURT: I get that, but I have to prepare for all eventualities.

MR. KLEIN: We understand, your Honor.

The second thing is that on April 4 the government filed a CIPA notice, Section 4 notice. It's docket number 36.

THE COURT: Yes.

MR. KLEIN: We would object to that, and we would ask for a Section 2 *ex parte* presentation to your Honor. I am not sure your Honor has finished your determination of what you have received.

THE COURT: I thought I had, but let me do this. Let me put on my docket that when my current trial is over, we will

reach out to you for a Section 2 hearing.

MR. KLEIN: Yes, your Honor. And we would like to make a request now that it be done virtually, since we are in Los Angeles, if possible.

THE COURT: That's complicated. Because when I have done the Section 2 hearings, they have been in a classified space, and I don't know how to get you in there in a nonelectronic format. So perhaps I can have only a subset of the team, or perhaps Mr. Patton can convey your thoughts.

MR. KLEIN: Yes, your Honor. We will figure it out.

THE COURT: So know that when I complete the civil trial we will reach out to you.

MR. KLEIN: Yes, your Honor.

THE COURT: Anything else, sir? Was there something else?

MR. KLEIN: Nothing from the defense.

THE COURT: Thank you all for a great oral argument today. Have a great weekend. I will talk to you when I can.

(Adjourned)